Moxa AirWorks AWK-4121
User's Manual

First Edition, January 2009

www.moxa.com/product

© 2009 Moxa Inc. All rights reserved.
Reproduction without permission is prohibited.

Moxa AirWorks AWK-4121
User's Manual

The Moxa software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright © 2009 Moxa Inc.
All rights reserved.
Reproduction without permission is prohibited.

Trademarks

MOXA is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use. This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information
www.moxa.com/support

Moxa Americas:
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office):
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-10-6872-3958

Moxa Europe:
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific:
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

Chapter 1 Introduction 1-1

Overview 1-2
Package Checklist 1-2
Product Features 1-2
Product Specifications 1-3
Functional Design 1-5
- LED Indicators 1-5
- Beeper 1-6
- Reset Button 1-6
- Relay (Digital Output) 1-7

Chapter 2 Getting Started 2-1

First-time Installation and Configuration 2-2
Communication Testing 2-3
Function Guide 2-4

Chapter 3 Web Console Configuration 3-1

Configuration by Web Browser 3-2
Overview 3-4
Basic Settings 3-5
- System Info Settings 3-5
- Network Settings 3-6
- Time Settings 3-7

Wireless Settings 3-8
- Basic Wireless Settings 3-8
- WLAN Security Settings 3-12
- Advanced Wireless Settings 3-20
- WLAN Certification Settings **(for EAP-TLS in Client mode only)** 3-21

Advanced Settings 3-22
- DHCP Server **(for AP mode only)** 3-22
- Packet Filters 3-24
- RSTP Settings **(for AP mode only)** 3-27
- SNMP Agent 3-29

Auto Warning Settings 3-31
- System Log 3-31
- Syslog 3-32
- E-mail 3-33
- Relay 3-34
- Trap 3-35

Status 3-36
- Associated Client List (for AP mode only) 3-36
- DHCP Client List (for AP mode only) 3-36
- System Log 3-37
- Relay Status 3-37
- DI and Power Status 3-38
- Wireless Status 3-38

Maintenance 3-38
- Console Settings 3-39
- Ping 3-39

Firmware Upgrade 3-40
Config Import Export 3-40
Load Factory Default 3-41
Password 3-41
Save Configuration 3-41
Restart 3-42
Logout 3-43

Chapter 4 Other Console Configurations 4-1
RS-232 Console Configuration (115200, None, 8, 1, VT100) 4-2
Configuration by Telnet and SSH Consoles 4-4
Configuration by Web Browser with HTTPS/SSL 4-5
Disabling Telnet and Browser Access 4-7

Chapter 5 References 5-1
Wireless Distribution System (WDS) 5-2
Beacon 5-4
DTIM 5-4
Fragment 5-4
RTS Threshold 5-4
STP and RSTP 5-4
The STP/RSTP Concept 5-4
Differences between RSTP and STP 5-5

Chapter 6 Supporting Information 6-1
About This User's Manual 6-2
DoC (Declaration of Conformity) 6-3
Federal Communication Commission Interference Statement 6-3
R&TTE Compliance Statement 6-3
Firmware Recovery 6-4
Technical Support Contact Information 6-5

1

Introduction

Moxa AirWorks AWK-4121 enables wireless access to network resources. The AWK-4121 is rated to operate at temperatures ranging from -40 to 75°C and is rugged enough for any harsh industrial environment.

In this chapter, we cover the following topics:

- **Overview**
- **Package Checklist**
- **Product Features**
- **Product Specifications**
- **Functional**
  - LED Indicators
  - Beeper
  - Reset Button
  - Relay (Digital Output)

Overview

The AWK-4121 outdoor wireless AP/bridge/client is an ideal 3-in-1 solution for industrial applications that are hard to wire, too expensive to wire, or use mobile equipment that connect to a TCP/IP network.

The AWK-4121 is rated to operate at temperatures ranging from -40 to 75°C, and its dust-tight and weatherproof design is IP67-rated. An IP67 rating means the device is completely protected from dust and is protected against the effects of immersion in water between 15cm and 1m in depth. This means you can set up a WLAN or extend existing wired networks to outdoor locations and still maintain a reliable connection. The AWK-4121 has two redundant DC power inputs for increased reliability, can be powered via PoE, and is easy to deploy.

Package Checklist

Moxa's AWK-4121 is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- 1 AWK-4121
- 2 Omni-directional antennas (5dBi, N-type male, 2.4 GHz)
- 1 Quick Installation Guide
- 1 Software CD
- 1 Moxa Product Warranty Booklet
- 1 Accessory Pack (including wall-mounting kit, screws and RJ45 field installable plug)

NOTE

The above items come with the AWK-4121 standard version. The package contents may vary in different customized versions.

Product Features

- IEEE802.11a/b/g Compliant
- Three-in-one design (AP/Bridge/Client)
- Advanced Wireless Security:
  - 64-bit and 128-bit WEP/WPA/WPA2
  - SSID Hiding/IEEE 802.1X/RADIUS
  - Packet access control & filtering
- STP/RSTP support for redundancy of system networking
- RS-232 console management
- 2DI+1DO for on-site monitoring and warming
- Free firmware update for more advanced functions
- Operating temperature ranges from -40 to 75℃
- Power input by redundant 24 VDC power inputs or Power over Ethernet
- Wall mounting ability

- IP67-rated metal housing

Product Specifications

WLAN

Standards	IEEE 802.11a/g/b for Wireless LAN IEEE 802.11i Wireless Security IEEE 802.3u 10/100BaseT(X) for Ethernet LAN EEE 802.3af for Power-over-Ethernet IEEE 802.1D/w STP/RSTP
Spread Spectrum and Modulation (Typical)	802.11b: DSSS with DBPSK, DQPSK, CCK 802.11g: OFDM with BPSK, QPSK, 16QAM, 64QAM 802.11a: OFDM with BPSK, QPSK, 16QAM, 64QAM
Operating Channels	US: 2.412 to 2.462 GHz (11 channels) 5.15 to 5.25 GHz (4 channels) EU: 2.412 to 2.472 GHz (13 channels) 5.15 to 5.25 GHz (4 channels) JP: 2.412 to 2.472 GHz (13 channels, OFDM) 2.412 to 2.484 GHz (14 channels, CCK) 5.15 to 5.25 GHz (4 channels for W52)
Security	64-bit and 128-bit WEP encryption, WPA /WPA2 (IEEE 802.1X/ RADIUS, TKIP and AES)
Protocol	General Protocols: Proxy ARP, DNS, HTTP, HTTPS, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, RTP AP-only Protocols: ARP, BOOTP, DHCP, dynamic VLAN-Tags for 802.1X-Clients, STP/RSTP (IEEE 802.1D/w)
Data Rates	802.11b: 1, 2, 5.5, 11 Mbps 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
Transmit Power	802.11b: 1 to 11 Mbps: Typ. 18±1.5 dBm 802.11g: 6 to 24 Mbps: Typ. 18±1.5 dBm 36 to 48 Mbps: Typ. 16±1.5 dBm 54 Mbps: Typ. 15±1.5 dBm 802.11a: 6 to 24 Mbps: Typ. 16±1.5 dBm 36 to 48 Mbps: Typ. 14±1.5 dBm 54 Mbps: Typ. 13±1.5 dBm≥17dBm
Receiver Sensitivity	802.11b: -92 dBm @ 1 Mbps, -90 dBm @ 2 Mbps, -88 dBm @ 5.5 Mbps, -84dBm @ 11 Mbps 802.11g: -87 dBm @ 6 Mbps, -86 dBm @ 9 Mbps, -85 dBm @ 12 Mbps, -82dBm @ 18 Mbps, -80 dBm @ 24 Mbps, -76 dBm @ 36 Mbps, -72dBm @ 48 Mbps, -70 dBm @ 54 Mbps 802.11a: -87 dBm @ 6 Mbps, -86 dBm @ 9 Mbps, -85 dBm @ 12 Mbps, -82dBm @ 18 Mbps, -80 dBm @ 24 Mbps, -76 dBm @ 36 Mbps, -72dBm @ 48 Mbps, -70 dBm @ 54 Mbps

Interface

Antenna Connector	N-type (female)
DI/DO Connection	8-pole M12 connector
Alarm Contact	1 relay output (capacity: 1A @24VDC)
Digital Input	2 electrically-isolated inputs • 0 to 3.3V for state "0" (OFF)

	• 10 to 48V for state "1" (ON) • Max. input current: 8 mA
Console	RS-232 (RJ45 type)
LAN Port	10/100BaseT(X) auto negotiation speed
LED Indicators	PWR, FAULT, STATE, WLAN and LAN

Power

Input Voltage	12 to 48 VDC, redundant dual DC power inputs or 48 VDC Power-over-Ethernet (IEEE 802.3af)
Input Current	0.494 to 0.121 A
Input Current (@ 24VDC)	0.3 A
Overload Current Protection	1.6 A
Reverse Polarity Protection	Present

Mechanical

Dimensions	224 x 147.7 x 66.5 mm (8.82 x 5.82 x 2.62 in)
Weight	1.2 kg
Installation	Wall Mounting or DIN-Rail (with optional wall mounting kit)
Casing	IP67 protection, aluminum case

Environment

Operating Temperature:	-40 to 75°C (-40 to 167°F)
Storage Temperature:	-40 to 85ºC (-40 to 185ºF)
Ambient Relative Humidity	5 to 95% (non-condensing)

Regulatory Approvals*

Radio:	EN300 328/ EN301 893/ EN301 489-1/-17 ARIB STD-33/T66/T71 (Japan)
EMI:	FCC Part 15

* Please check Moxa's website for the most up-to-date certification status.

Warranty 5 years

Details: See http://*www.moxa.com/warranty*

ATTENTION

The AWK-4121 is NOT a portable mobile device and should be located at least 20cm away from the human body.

Functional Design

LED Indicators

The LEDs on the front panel of AWK-4121 allow you to identity the status and wireless settings quickly.

The LED for **FAULT** indicates the system failure and user-configured events. If the AWK-4121 cannot retrieve the IP address from a DHCP server, the **FAULT** LED will blink at an interval of one second.

The following table is a summary for the wireless settings and LED displays. You can check the status of the AWK-4121 by reading these LEDs. More information about "Basic Wireless Settings" is presented in Chapter 3.

LED	Color	State	Description
PWR	Green	On	Power is being supplied (from power input 1 or 2, or PoE).
		Off	Power is **not** being supplied
FAULT	Red	On	Relay is event-triggered.
		Blink (slow)	Cannot get an IP address from the DHCP server (interval: 1 sec)
		Blink (fast)	IP address conflict (interval: 0.5 sec)
		Off	Normal status
STATE	Green/Red	Green	Software Ready
		Green Blink	The AWK Search Utility has located the AWK. (interval: 1sec)
		Red	Booting or Error condition
WLAN	Green/Amber	Green On	WLAN functions in **Client** mode.
		Green Blink	WLAN's data communication is run in **Client** mode
		Amber On	WLAN functions in **AP/Bridge** mode.
		Amber Blink	WLAN's data communication is run in **AP/Bridge** mode
		Off	WLAN is not in use or not working properly.
LAN	Yellow/ Green	Yellow On	LAN port's 10Mbps link is active.
		Yellow Blink	Data is being transmitted at 10 Mbps
		Yellow Off	LAN port's 10Mbps link is inactive.
		Green On	LAN port's 100Mbps link is active.
		Green Blink	Data is being transmitted at 100 Mbps
		Green Off	LAN port's 100Mbps link is inactive.

ATTENTION

When the LEDs for **STATE** (Green), **FAULT**, and **WLAN** all light up simultaneously and blink at one-second intervals, it means the system failed to boot. This may be due to improper operation or uncontrollable issues, such as an unexpected shutdown during firmware update. To recover the firmware, refer to "Firmware Recovery" in Chapter 6.

Beeper

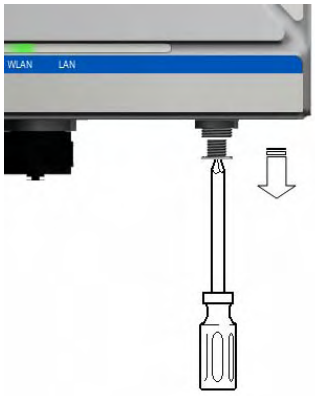
The beeper signals that the system is ready with two short beeps.

Reset Button

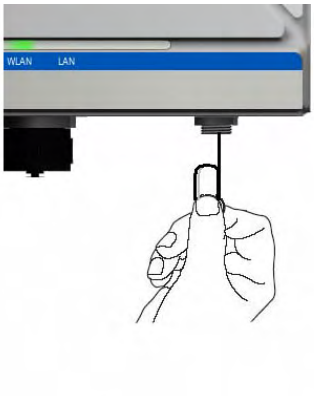
The **RESET** button is located on the bottom panel of the AWK-4121. You can reboot the AWK-4121 or reset it to factory default settings by pressing the **RESET** button with a pointed object such as an unfolded paper clip.

- **System reboot:** Hold the RESET button down for *under* 5 seconds and then release.
- **Reset to factory default:** Hold the RESET button down for *over* 5 seconds until the **STATE** LED starts blinking green. Release the button to reset the AWK-4121.

STEP 1: Remove the reset button cover.



STEP 2: Using a pointed object, press and hold the reset button.



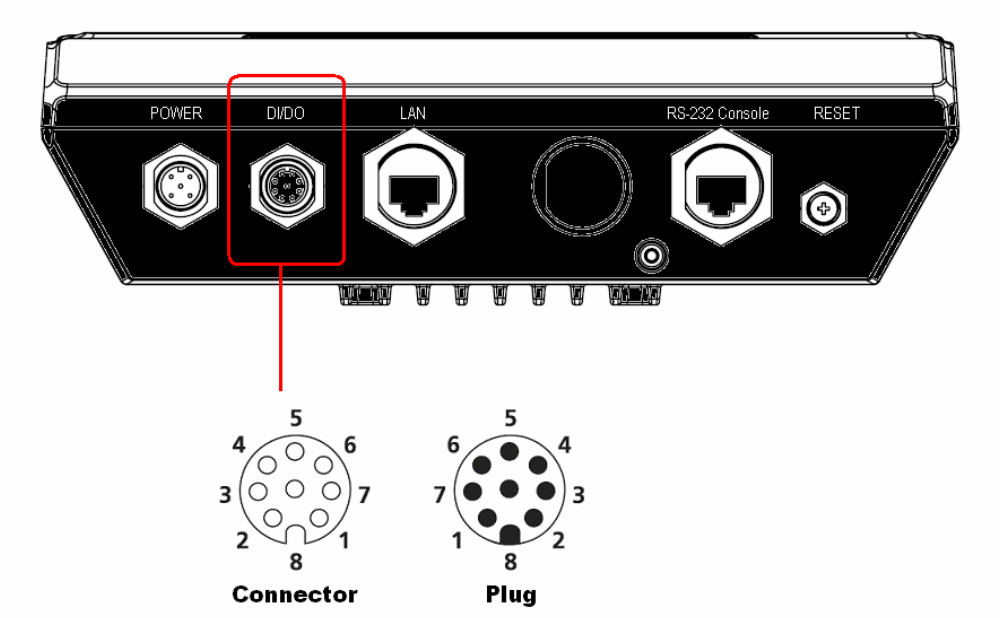
Relay (Digital Output)

The AWK-4121 has one relay output, which consists of the 2 contacts for the 8-pin M12 connector on the bottom panel, as shown below. These relay contacts forward system failure and user-configured events.

The two wires attached to the relay contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the relay circuit will remain closed. For safety reason, the relay circuit is kept open when the AWK-4121 is not powered.

The AWK-4121's relay status is summarized as follows:

Relay Status	Power off	Power on
No Event	**OPEN**	**CLOSED**
Triggered		**OPEN**



Digital Inputs and Relay-out Pin Assignment (8-pin M12 connector)

PIN	1	2	3	4	5	6	7	8
Function	DOUT_I	DOUT_O	DI0+	DI0-	DI1+	DI1-	reserved	reserved

2

Getting Started

This chapter explains how to install Moxa's AirWorks AWK-4121 for the first time, quickly set up your wireless network, and test whether the connection is running well. With the function guide, you can easily locate the functions you need.

In this chapter, we cover the following topics:

- **First-time Installation and Configuration**
- **Communication Testing**
- **Function Guide**

First-time Installation and Configuration

Before installing the AWK-4121, make sure all items in the Package Checklist are in the box. In addition, you will need access to a notebook computer or PC equipped with an Ethernet port. The AWK-4121 has a default IP address that you must use when connecting to the device for the first time.

Step 1: Select the power source.

The AWK-4121 can be powered by DC power input or PoE (Power over Ethernet). The AWK-4121 will use whichever power source you choose.

Step 2: Connect the AWK-4121 to a notebook or PC.

Since the AWK-4121 supports MDI/MDI-X auto-sensing, you can use either a straight-through cable or crossover cable to connect the AWK-4121 to a computer. If the LED indicator on AWK-4121's LAN port lights up, it means the connection is established.

Step 3: Set up the computer's IP address.

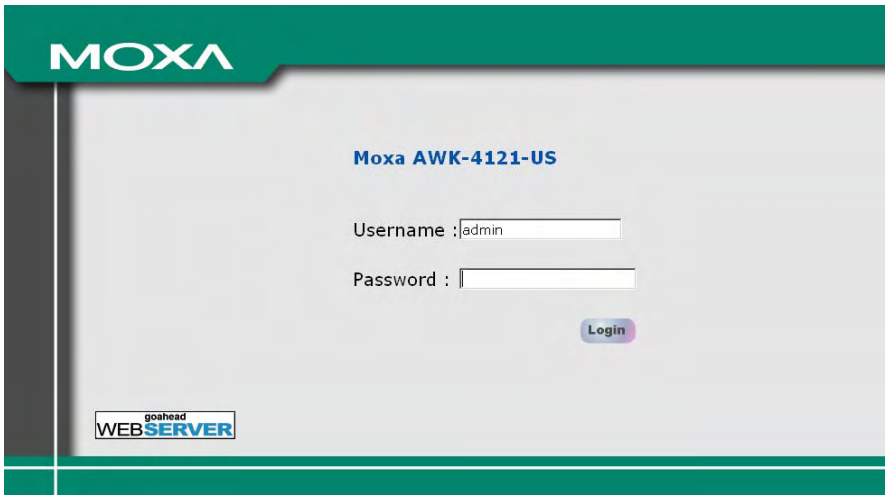
Set an IP address on the same subnet as the AWK-4121. Since the AWK-4121's default IP address is **192.168.127.253**, and the subnet mask is **255.255.255.0**, you should set the IP address of the computer to **192.168.127.xxx**.

NOTE

After you select **Maintenance** → **Load Factory Default** and click the **Submit** button, the AWK-4121 will be reset to factory default settings and the IP address will be also reset to **192.168.127.253**.

Step 4: Use the web-based manager to configure AWK-4121

Open your computer's web browser and type http://192.168.127.253 in the address field to access the homepage of the web-based Network Manager. Before the homepage opens, you will need to enter the user name and password as shown in the following figure. For first-time configuration, enter the default user name and password and then click on the **Login** button:



NOTE

Default user name and password:

User Name: **admin**

Password: **root**

For security reasons, we strongly recommend changing the default password. To do so, select **Maintenance** > **Password**, and then follow the on-screen instructions to change the password.

NOTE

Clicking **Submit** will apply your changes refresh the web page. The string "**(Config Setting Success)**" and a blinking reminder will appear in the upper-right corner of web page, as follows.

MOXA www.moxa.com
** Click Restart to activate new settings! **
Total Solution for Industrial Wireless Networking
Main Menu
Overview
System Info Settings (Config Setting Success)

To make the changes effective, click **Restart** and then **Save and Restart** after you change the settings. It will take about 30 seconds for the AWK-4121 to restart.

Step 5: Select the operation mode for the AWK-4121.

By default, the AWK-4121's operation mode is set to AP. You can change the setting in **Wireless Settings → Basic Wireless Settings** if you would like to use the Client mode instead. Detailed information about configuring the AWK-4121's operation can be found in Chapter 3.

Step 6: Test communications.

We will describe 2 test methods to make sure the network connection has been established. Please refer to the following section for more details.

Communication Testing

After installation, you can run a sample test to make sure the AWK-4121 and wireless connection are functioning normally. Two testing methods are explained in the following sections. Use the first method if you are using only one AWK-4121 device, and use the second method if you are using two or more AWK-4121s.

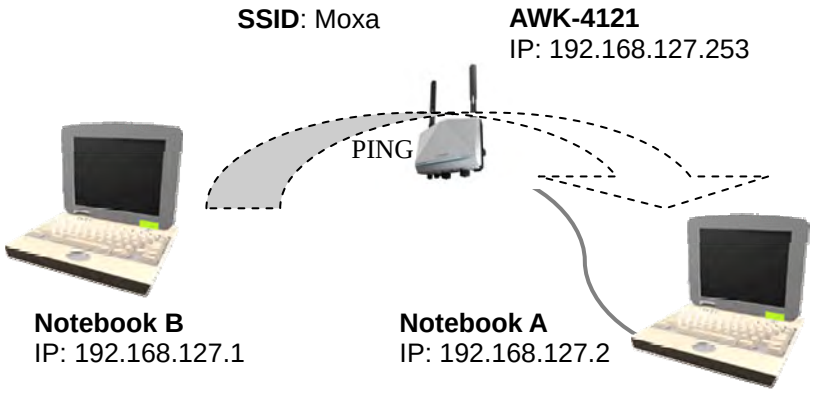
Testing Method for one AWK-4121

If you are only using one AWK-4121, you will need a second notebook computer equipped with a WLAN card. Configure the WLAN card to connect to the AWK-4121 (NOTE: the default SSID is **MOXA**), and change the IP address of the second notebook (B) so that it is on the same subnet as the first notebook (A), which is connected to the AWK-4121.

After configuring the WLAN card, establish a wireless connection with the AWK-4121 and open a DOS window on Notebook B. At the prompt, type

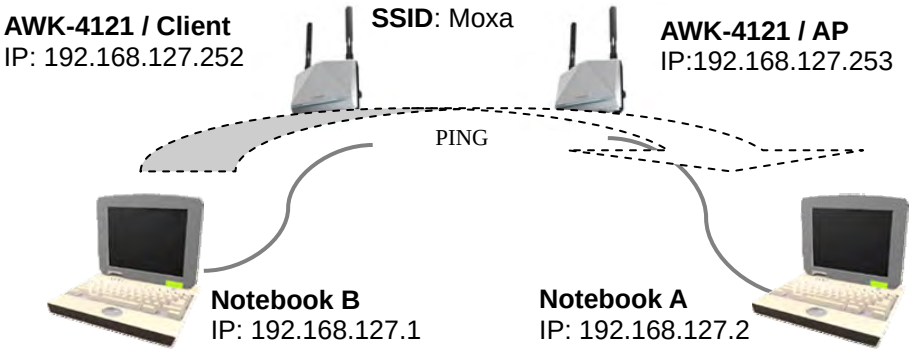
ping <*IP address of notebook A*>

and then press **Enter** (see the figure below). A "Reply from IP address …" response means the communication was successful. A "Request timed out." response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.



Testing Method for two or more AWK-4121s

If you have two or more AWK-4121s, you will need a second notebook computer (B) equipped with an Ethernet port. Use the default settings for the first AWK-4121 connected to notebook A and change the second or third AWK-4121 connected to notebook B to Client mode. Then, configure the notebooks and AWK-4121s properly.



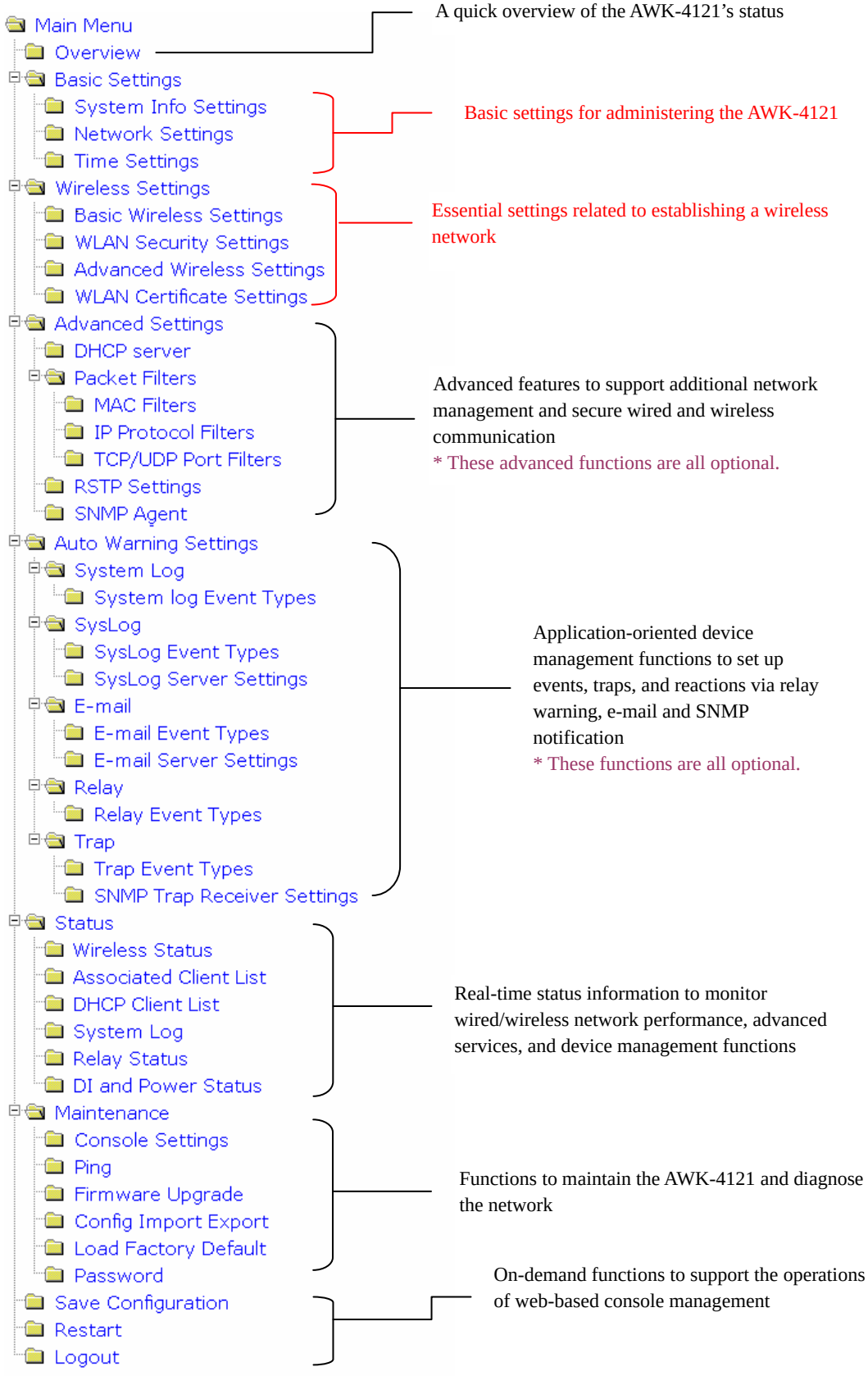
After setting up the testing environment, open a DOS window on notebook B. At the prompt, type

ping <*IP address of notebook A*>

and then press **Enter**. A "Reply from IP address …" response means the communication was successful. A "Request timed out" response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.

Function Guide

The management functions are categorized in a tree and shown in the left field of the web-based management console. You can efficiently locate the function you need with the following guide.


Main Menu
Overview
Basic Settings
System Info Settings
Network Settings
Time Settings
Wireless Settings
Basic Wireless Settings
WLAN Security Settings
Advanced Wireless Settings
WLAN Certificate Settings
Advanced Settings
DHCP server
Packet Filters
MAC Filters
IP Protocol Filters
TCP/UDP Port Filters
RSTP Settings
SNMP Agent
Auto Warning Settings
System Log
System log Event Types
SysLog
SysLog Event Types
SysLog Server Settings
E-mail
E-mail Event Types
E-mail Server Settings
Relay
Relay Event Types
Trap
Trap Event Types
SNMP Trap Receiver Settings
Status
Wireless Status
Associated Client List
DHCP Client List
System Log
Relay Status
DI and Power Status
Maintenance
Console Settings
Ping
Firmware Upgrade
Config Import Export
Load Factory Default
Password
Save Configuration
Restart
Logout
A quick overview of the AWK-4121's status
Basic settings for administering the AWK-4121
Essential settings related to establishing a wireless network
Advanced features to support additional network management and secure wired and wireless communication
* These advanced functions are all optional.
Application-oriented device management functions to set up events, traps, and reactions via relay warning, e-mail and SNMP notification
* These functions are all optional.
Real-time status information to monitor wired/wireless network performance, advanced services, and device management functions
Functions to maintain the AWK-4121 and diagnose the network
On-demand functions to support the operations of web-based console management

3

Web Console Configuration

In this chapter, we will explain each web management page of the web-based console configuration. Moxa's easy-to-use management functions will help you set up your AWK-4121, as well as establish and maintain your wireless network easily.

In this chapter, we cover the following topics:

- **Configuration by Web Browser**
- **Overview**
- **Basic Settings**
- **Wireless Settings**
- **Advanced Settings**
- **Auto Warning Setting**
- **Status**
- **Maintenance**
- **Save Configuration**
- **Restart**
- **Logout**

Configuration by Web Browser

Moxa AWK-4121's web browser interface provides a convenient way to modify its configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft® Internet Explorer 5.5 or 6.0 with JVM (Java Virtual Machine) installed.

NOTE

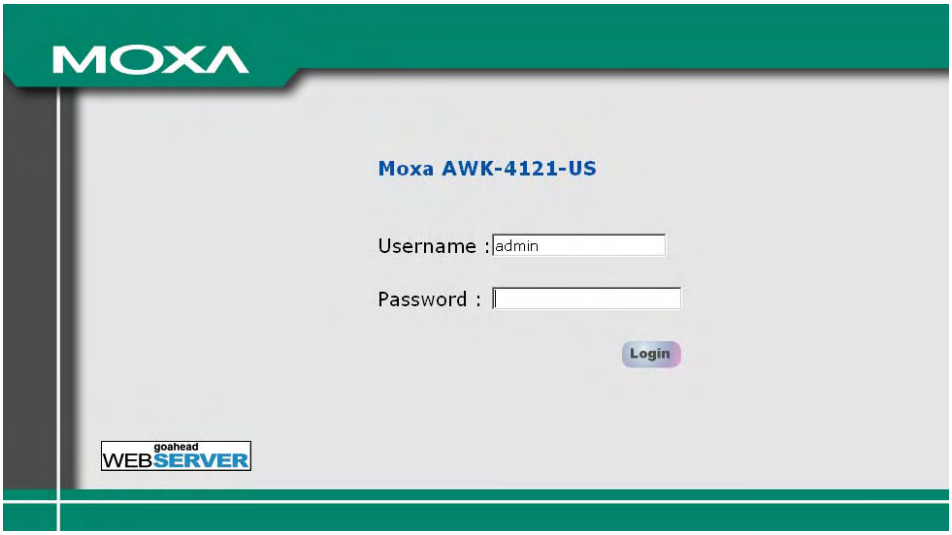
To use the AWK-4121's management and monitoring functions from a PC host connected to the same LAN as the AWK-4121, you must make sure that the PC host and AWK-4121 are on the same logical subnet. Similarly, if the AWK-4121 is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

The Moxa AWK-4121's default IP address is **192.168.127.253**.

Follow the steps below to access the AWK-4121's web-based console management.

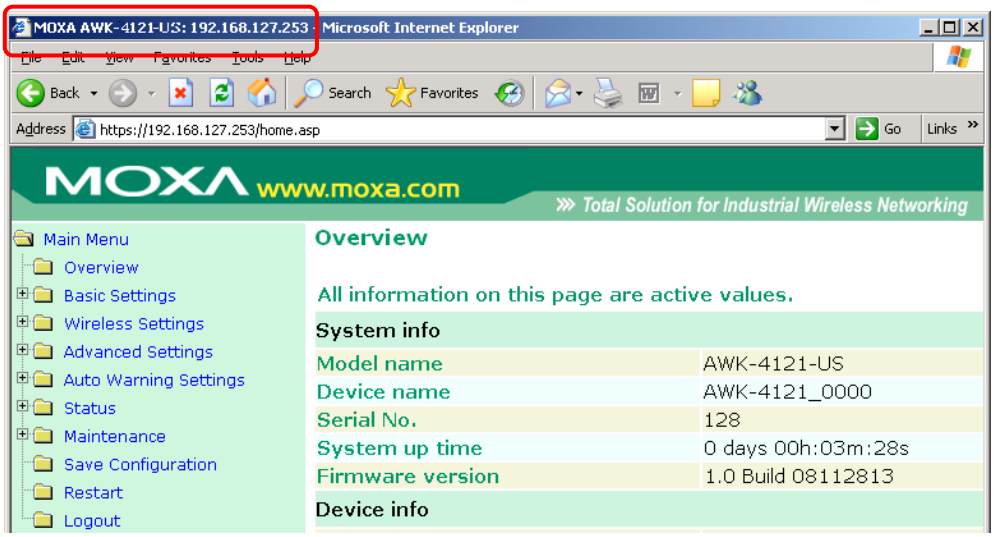
1. Open your web browser (ex. Internet Explorer) and type the AWK-4121's IP address in the address field. Then press **Enter** to establish the connection.

2. The Web Console Login page will open. Enter the password (User Name is set as **admin**; the default password is **root** if a new password has not been set.) and then click **Login** to continue.



You may need to wait a few moments for the web page to download onto your computer. Please note that the model name and IP address of your AWK-312 are both shown in the title of the web page. This information can help you identify multiple AWK-4121s.

You can use the menu tree on the left side of the window to open the function pages to access each of AWK-4121's functions.



In the following paragraphs, we will go through each of the AWK-4121's management functions in detail. You can also get a quick overview of these functions in the **Function Guide** section of Chapter 2.

NOTE

The model name of the AWK-4121 is shown as AWK-4121-XX where XX indicates the country code. The country code represents the AWK-4121 version and which bandwidth it uses. We use **AWK-4121-US** as an example in the following figures. The country code for the model name on your screen may vary if you are using a different version (band) AWK-4121.

Overview

The **Overview** page summarizes the AWK-4121's current status. The information is categorized into several groups: **System info**, **Device info** and **802.11 info**.

All information on this page are active values.

System info	
Model name	AWK-4121-US
Device name	AWK-4121_0000
Serial No.	0
System up time	0 days 00h:01m:32s
Firmware version	1.0 Build 08112813
Device info	
Device MAC address	00:90:E8:00:46:11
IP address	192.168.127.253
Subnet mask	255.255.255.0
Gateway	
802.11 info	
Operation mode	AP
Channel	6
SSID	MOXA
Security mode	Open
RF type	B/G Mixed
Current BSSID	N/A
Signal strength	N/A
Transmission rate	Auto
Country code	US

NOTE

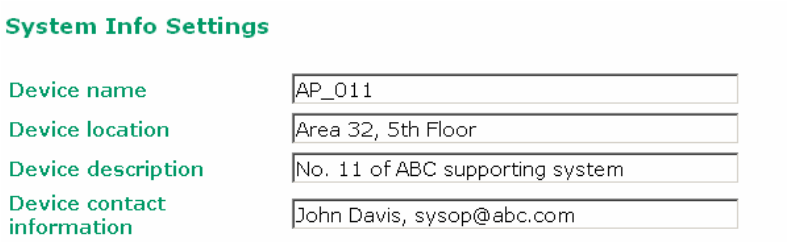
Some values for **802.11 info** may not show up due to different operation modes. For example **Current BSSID** and **RSSI** are not available in AP mode.

Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the AWK-4121.

System Info Settings

The **System Info** items, especially ***Device name*** and ***Device description***, are displayed and included on the **Overview** page, SNMP information, and alarm emails. Setting **System Info** items makes it easier to identify the different AWK-4121s connected to your network.



Device name

Setting	Description	Factory Default
Max. 31 Characters	This option is useful for specifying the role or application of different AWK-4121 units.	AWK-4121_*<Serial No. of this AWK-4121>*

Device location

Setting	Description	Factory Default
Max. 31 Characters	This specifies the location of different AWK-4121 units.	None

Device description

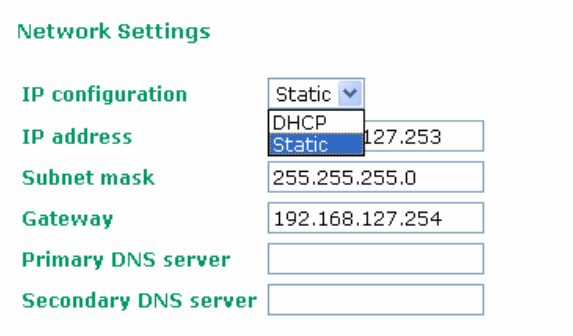
Setting	Description	Factory Default
Max. 31 Characters	Use this space to record more detailed description of AWK-4121.	None

Device name

Setting	Description	Factory Default
Max. 31 Characters	To provide information about whom to contact in order to resolve problems, use this space to record contact information of the person responsible for maintaining this AWK-4121.	None

Network Settings

The Network Settings configuration allows you to modify the usual TCP/IP network parameters. An explanation of each configuration item is given below.



IP configuration

Setting	Description	Factory Default
DHCP	The AWK-4121's IP address will be assigned automatically by the network's DHCP server	Static
Static	Set up the AWK-4121's IP address manually.	

IP address

Setting	Description	Factory Default
AWK-4121's IP address	Identifies the AWK-4121 on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
AWK-4121's subnet mask	Identifies the type of network to which the AWK-4121 is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

Gateway

Setting	Description	Factory Default
AWK-4121's default gateway	The IP address of the router that connects the LAN to an outside network.	None

NOTE

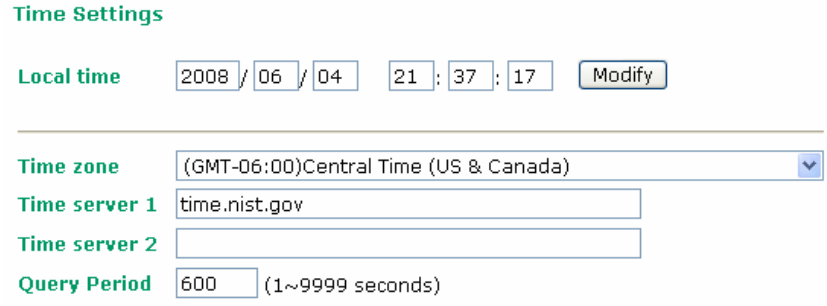
A warning message will be shown once to remind you to set up the default gateway if the ***Gateway*** is not set in **Client** mode. It is not necessary to set up a default gateway for the AWK-4121 if you only plan to establish a local network, and no packet goes to an outside network.

Primary/ Secondary DNS server

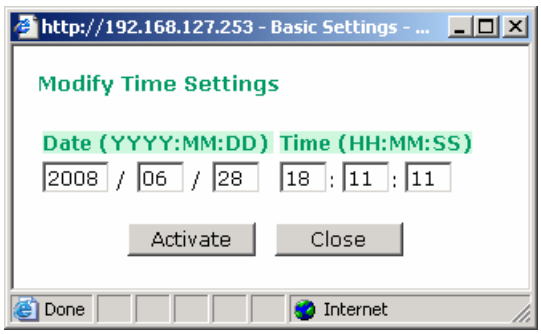
Setting	Description	Factory Default
IP address of Primary/ Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the AWK-4121's URL (e.g., *http://ap11.abc.com*) in your browser's address field instead of entering the IP address. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

Time Settings

The AWK-4121 has a time calibration function based on information from an NTP server or user specified Date and Time information. Functions such as Auto warning can add real-time information to the message.



You can click on the **Modify** button to initiate a time setting dialog box, as shown in the following figure. After setting the time and date parameters, you can click the **Activate** button to apply the setting or discard it by clicking **Close**. Local time settings will be immediately activated in the system without running Save and Restart.



NOTE

The AWK-4121 has a real time clock (RTC). Users are strongly recommended to update the **Local time** for the AWK-4121 after initial setup or long-term shutdown, especially when the network does not have an Internet connection for accessing the NTP server or there is no NTP server on the LAN.

Local time

Setting	Description	Factory Default
User adjustable time	The date and time parameters allow configuration of the local time with an interactive dialog box.	None (yyyy/mm/dd hh:mm:ss format; 24-hour format.)

Time zone

Setting	Description	Factory Default
User selectable time zone	The time zone setting allows conversion from GMT (Greenwich Mean Time) to local time.	GMT (Greenwich Mean Time)

ATTENTION

Changing the time zone will automatically adjust the current **Local time**. You should configure the **Time zone** before setting the **Local time**.

Time server 1/ 2

Setting	Description	Factory Default
The 1st/ 2nd time server IP/Name	IP or Domain address of NTP time server. The 2nd time will be used if the 1st NTP server fails to connect.	None

Query period

Setting	Description	Factory Default
Query period time (1- 9999 seconds)	This parameter determines how frequently the time is updated from the NTP server.	600 (seconds)

Wireless Settings

The essential settings for wireless networks are presented in this function group. Settings must be properly set before establishing your wireless network.

Basic Wireless Settings

The AWK-4121 mainly supports two operational modes that have distinct roles in the wireless network:

- **AP/Bridge:**

  This mode provides both Access Point and Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through the Wireless Distribution System (WDS).

- **AP Client:**

  This mode is for Dynamic LAN-to-LAN Bridging or Device-to-LAN. The AP Client automatically establishes bridge links with other APs.

In either mode, the AWK-4121 forwards packets between its Ethernet interface (LAN) and wireless interface (WLAN) for wired hosts on the Ethernet side and wireless host(s) on the wireless side. There are two types of wireless links as specified by the IEEE802.11 standard:

- **STA-AP**

  This type of wireless link is established between an IEEE802.11 Station (STA) and an IEEE802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC). The Client mode is actually an STA.

- **WDS**

  This type of wireless link is established between two IEEE802.11 APs. Wireless packets transmitted along the WDS link comply with the IEEE802.11 WDS (Wireless Distribution System) format at the link layer. You can refer to "Wireless Distribution System (WDS)" in Chapter 5 for more details. Be reminded that WPA/WPA2 **CANNOT** be supported in WDS.

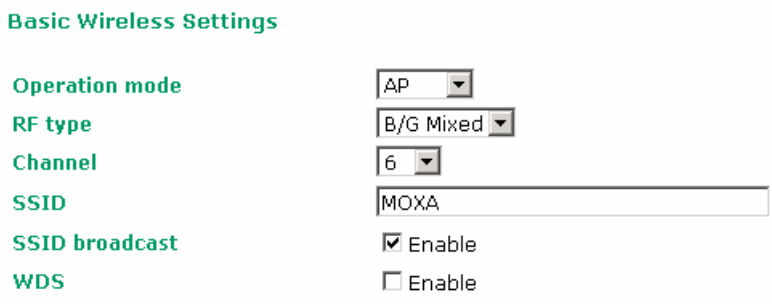
To establish a static bridge link based on the WDS, the APs at both end of the WDS link must be configured manually with each other's MAC addresses. To establish a dynamic bridge link between an AP and a Client, both devices must be configured with the same, channel, and security settings (see "WLAN Security Settings"). Moreover, the same SSID is also needed if a client will roam along the APs in Bridge mode. The AP Client automatically scans for any AP that is using the matched SSID and establishes a bridge link with the scanned AP.

When the AWK-4121 is configured to be in **Client** mode, it can be used as an Ethernet-to-wireless (or LAN-to-WLAN) network adapter. For example, a notebook computer equipped with an Ethernet adapter, but no wireless card, can be connected to this device with an Ethernet cable for wireless connectivity to another AP.

NOTE

Although it is more convenient to use dynamic bridging, there is a limitation — the AP Client can only transmit IP-based packets between its wireless interface (WLAN) and Ethernet interface (LAN); other types of traffic (such as IPX and AppleTalk) are not forwarded.

The following figure shows the Basic Wireless Settings page. The parameters and options are described as follow:

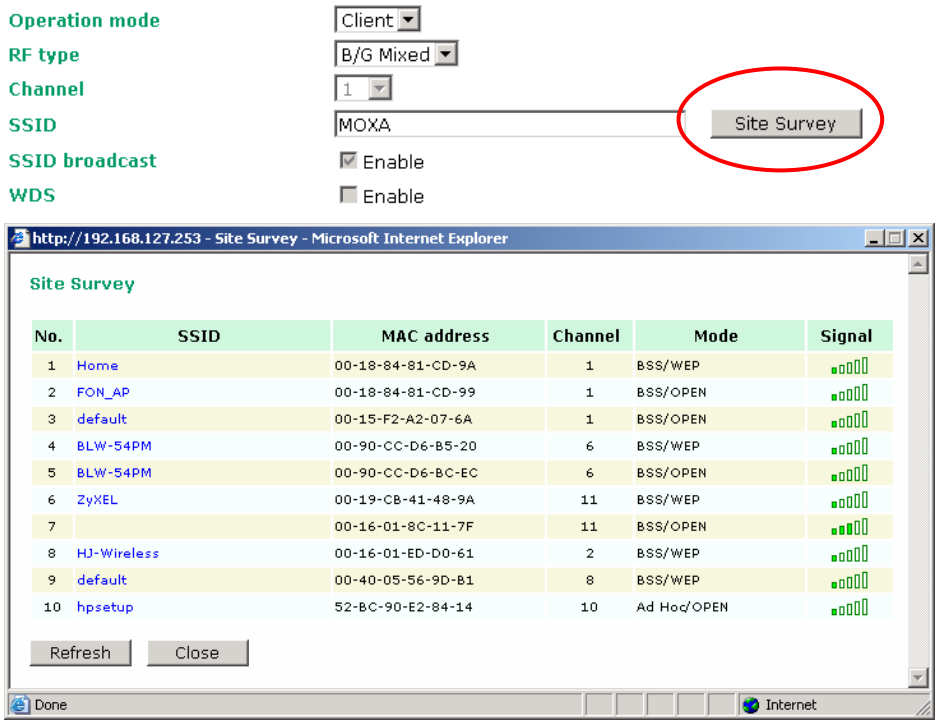


Operation mode

Setting	Description	Factory Default
AP	AWK-4121 plays a role of wireless AP/ Bridge.	AP
Client	AWK-4121 plays a role of wireless AP Client.	

NOTE

When you switch to **Client** mode, you can find an additional **Site Survey** button on this page. It can support site survey and pop up a dialog box listing the information of available APs, as shown in the following figure. You can click on the SSID of an entity and bring the value of its SSID onto the SSID field of the Basic Wireless Settings page. Clicking on the **Refresh** button will re-scan and update the table.



NOTE

If the **Gateway** field in **Basic Settings > Network Settings** is empty, a warning message will appear, reminding you to set the default gateway when **Client** mode is enabled. You can ignore this message if you are only planning a local network and no packets will be sent outside the network.

RF type

Setting	Description	Factory Default
A	Supports IEEE802.11a standard only	B/G Mixed
B	Supports IEEE802.11b standard only	
G	Supports IEEE802.11g standard only	
B/G Mixed	Supports both of IEEE802.11b/g standards, but 802.11g can be slowed down when 802.11b clients are on the network	

***Channel* (for AP mode only)**

Setting	Description	Factory Default
Available channels vary with RF type	AWK-4121 plays a role of wireless AP.	6 (in B/G Mixed mode)

SSID

Setting	Description	Factory Default
Max. 31 Characters	The SSID of a client and the SSID of the AP must be identical for them to communicate with each other.	MOXA

***SSID broadcast* (for AP mode only)**

Setting	Description	Factory Default
Enable/ Disable	SSID can be broadcast or not.	Enable

NOTE

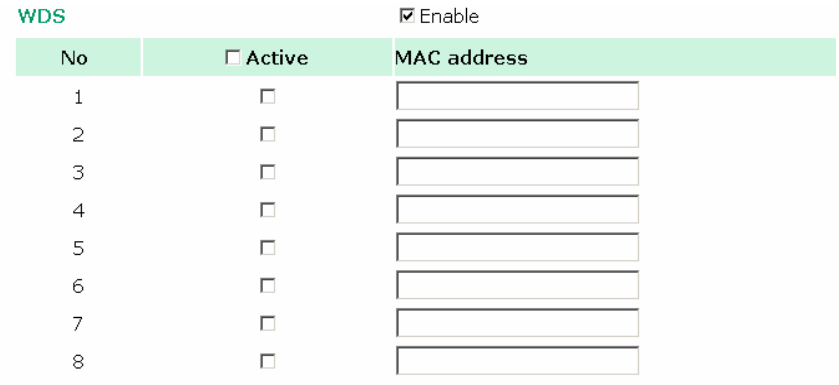
The AWK-4121-JP (for Japanese frequency bands) only connects SSID-hidden APs in all IEEE802.11a channels and IEEE802.11g channel 1 to 11. The AWK-4121-EU (for European frequency bands) only connects SSID-hidden APs in all IEEE802.11b/g channels.

***WDS* (for AP mode only)**

Setting	Description	Factory Default
Enable/ Disable	AWK-4121 supports WDS or not.	Disable

NOTE

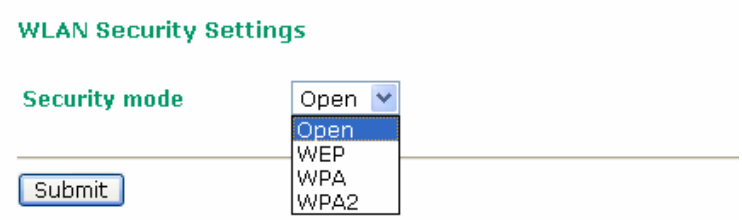
The AWK-4121 provides 8 entities for WDS settings and can support up to 8 WDS links to other APs or wireless bridges. The list appears when WDS **Enable** is checked. Enter the MAC address to set up a WDS link. Remember to activate a WDS link by checking the **Active** check box.



WLAN Security Settings

The AWK-4121 provides four standardized wireless security modes: Open, WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2. Several types of security models are available in AWK-4121 by selecting ***Security mode*** and ***WPA type***:

- **Open**: No authentication, no data encryption.
- **WEP**: Static WEP (Wired Equivalent Privacy) keys must be manually configured.
- **WPA/WPA2-Personal**: Also known as WPA/WPA2-PSK. You need to specify the Pre-Shared Key in the ***Passphrase*** field, which will be used by the TKIP or AES engine as a master key to generate keys that actually encrypt outgoing packets and decrypt incoming packets.
- **WPA/WPA2-Enterprise**: Also called WPA/WPA2-EAP (Extensible Authentication Protocol). In addition to device-based authentication, WPA/WPA2-Enterprise enables user-based authentication via IEEE802.1X. The AWK-4121 can support three EAP methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.



Security mode

Setting	Description	Factory Default
Open	No authentication	Open
WEP	Static WEP is used	
WPA*	WPA is used	
WPA2*	Fully supports IEEE802.11i with "TKIP/AES + 802.1X"	

** WPA and WPA2 cannot be supported in WDS (Bridge) mode.*

Open

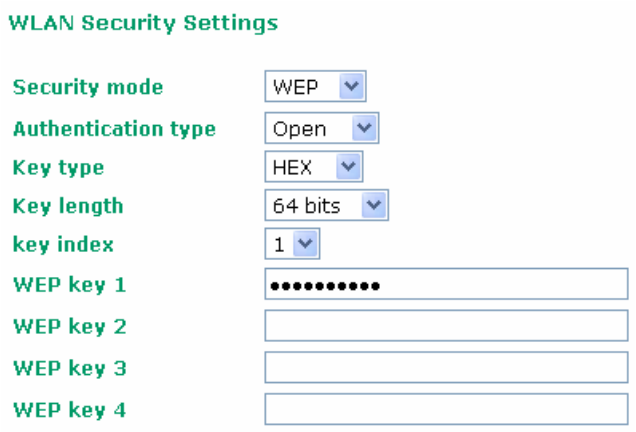
For security reasons, it is highly recommended that the security mode should be set to the options other than Open System. When the security mode is set to Open System, no authentication or data encryption will be performed.

WEP

According to the IEEE802.11 standard, WEP can be used for authentication and data encryption (confidentiality). **Shared** (or **Shared Key**) authentication type is used if WEP authentication and data encryption are both needed. Normally, **Open** (or **Open System**) authentication type is often used when WEP data encryption is run with authentication.

When WEP is enabled as a security mode, the length of a key (so-called WEP seed) can be specified as 64/128 bits, which is actually a 40/104-bit secret key with a 24-bit initialization vector. The AWK-4121 provides 4 entities of WEP key settings that can be selected to use with ***Key index***. The selected key setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

The WEP key can be presented in two ***Key type***, HEX and ASCII. Each ASCII character has 8 bits, so a 40-bit (or 64-bit) WEP key contains 5 characters, and a 104-bit (or 128-bit) key has 13 characters. In hex, each character uses 4 bits, so a 40-bit key has 10 hex characters, and a 128-bit key has 26 characters.



Authentication type

Setting	Description	Factory Default
Open	Data encryption is enabled, but no authentication	Open
Shared	Data encryption and authentication are both enabled.	

Key type

Setting	Description	Factory Default
HEX	Specifies WEP keys in hex-decimal number form	HEX
ASCII	Specifies WEP keys in ASCII form	

Key length

Setting	Description	Factory Default
64 bits	Uses 40-bit secret keys with 24-bit initialization vector	64 bits
128 bits	Uses 104-bit secret key with 24-bit initialization vector	

Key index

Setting	Description	Factory Default
1-4	Specifies which WEP key is used	Open

WEP key 1-4

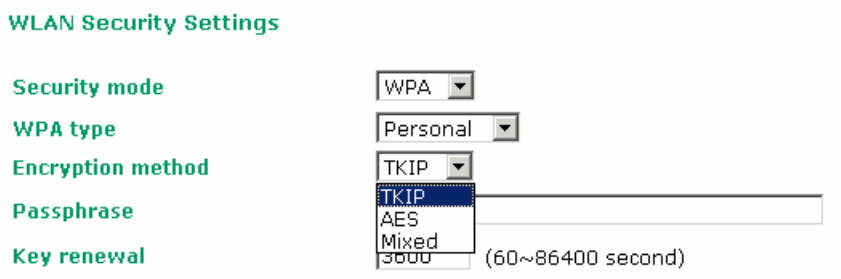
Setting	Description	Factory Default
ASCII type: 64 bits: 5 chars 128 bits: 13chars HEX type: 64 bits: 10 hex chars 128 bits: 26 hex chars	A string that can be used as a WEP seed for RC4 encryption engine.	None

WPA/WPA2-Personal

WPA (Wi-Fi Protected Access) and WPA2 are significantly improved encryption methods of WEP. WPA is a security standard based on 802.11i draft 3, while WPA2 is based on the fully ratified version of 802.11i. The initial vector is transmitted, encrypted, and enhanced with its 48 bits, twice as long as WEP. The key is regularly changed so for added security.

Even though AES encryption is only included in the WPA2 standard, it is widely available in the WPA security mode of some wireless APs and clients as well. The AWK-4121 also supports AES algorithms in WPA and WPA2 for better compatibility.

Personal versions of WPA/WPA2, also know as WPA/WPA-PSK (*Pre-Shared Key*), provides a simple way of encrypting a wireless connection for high confidentiality. A ***Passphrase*** is used as a basis for encryption methods (or cipher types) in a WLAN connection. The passphrases should be complex and as long as possible. The number of ASCII characters of the Passphrase must be at least 8 and can go up to 63. For security reason, this passphrase should be disclosed to the relevant users only and changed regularly.



WPA type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2	

Encryption method

Setting	Description	Factory Default
TKIP	**T**emporal **K**ey **I**ntegrity **P**rotocol is enabled	TKIP
AES	**A**dvance **E**ncryption **S**ystem is enabled	
Mixed*	Provides for both TKIP and AES **This option is available in AP mode only.*	

Passphrase

Setting	Description	Factory Default
8 – 63 characters	Master key to generate keys for encryption and decryption	None

***Key renewal* (for AP mode only)**

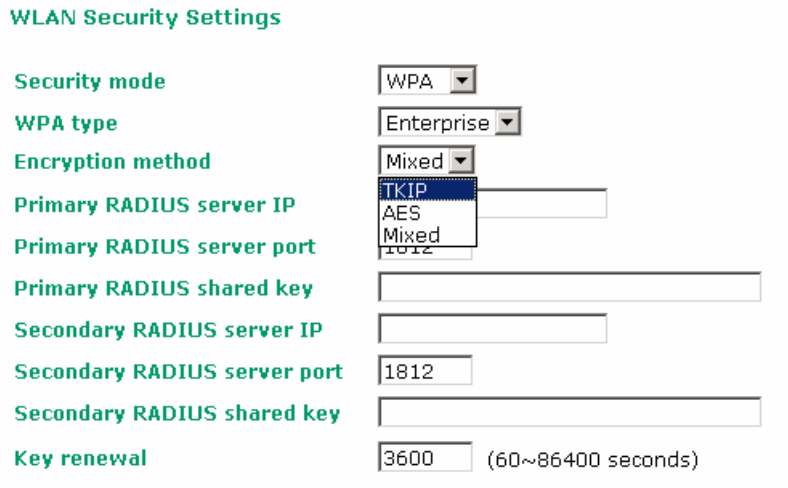
Setting	Description	Factory Default
60 – 86400 seconds (1 minute to 1 year)	Specifies the time period of group key renewal	3600 (seconds)

NOTE

The value for ***key renewal*** instructs the wireless AP how often it should change the encryption keys. Usually the security level will be higher if you set this value shorter so that the encryption keys are changed more often. Default value is 3600 seconds (6 minutes). Longer time periods can be considered if traffic is not so busy.

WPA/WPA2-Enterprise (for AP mode)

By selecting ***WPA type*** as **Enterprise**, you can use **EAP** (*Extensible Authentication Protocol*), a framework authentication protocol used by 802.1X to provide network authentication. In these Enterprise-level security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1X functionality is enabled in WPA /WPA2. The IEEE 802.1X protocol also offers the possibility of carrying out an efficient connection authentication in a large-scaled network. It is not necessary to exchange keys or passphrases.



WPA type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2	

Encryption method

Setting	Description	Factory Default
TKIP	**T**emporal **K**ey **I**ntegrity **P**rotocol is enabled	TKIP
AES	**A**dvance **E**ncryption **S**ystem is enabled	
Mixed	Provides for both TKIP and AES	

Primary/ Secondary RADIUS server IP

Setting	Description	Factory Default
The IP address of RADIUS server	Specifies the delegated RADIUS server for EAP	None

Primary/ Secondary RADIUS port

Setting	Description	Factory Default
Port number	Specifies the port number of the delegated RADIUS server	1812

Primary/ Secondary RADIUS shared key

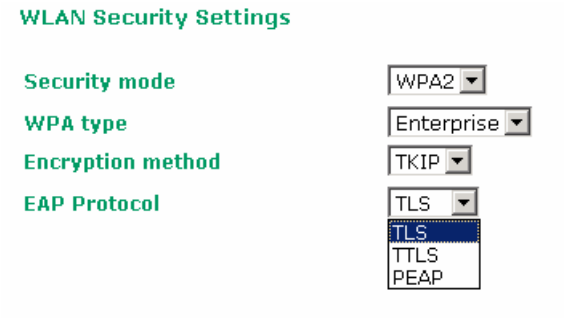
Setting	Description	Factory Default
Max. 31 characters	The secret key shared between AP and RADIUS server	None

Key renewal

Setting	Description	Factory Default
60 – 86400 seconds (1 minute to 1 year)	Specifies the time period of group key renewal	3600 (seconds)

WPA/WPA2-Enterprise (for Client mode)

In a client role, the AWK-4121 can support three EAP methods (or ***EAP protocol***s): **EAP-TLS**, **EAP-TTLS**, and **EAP-PEAP**, corresponding to WPA/WPA-Enterprise settings on the AP side.



Encryption method

Setting	Description	Factory Default
TKIP	**T**emporal **K**ey **I**ntegrity **P**rotocol is enabled	TKIP
AES	**A**dvance **E**ncryption **S**ystem is enabled	

EAP Protocol

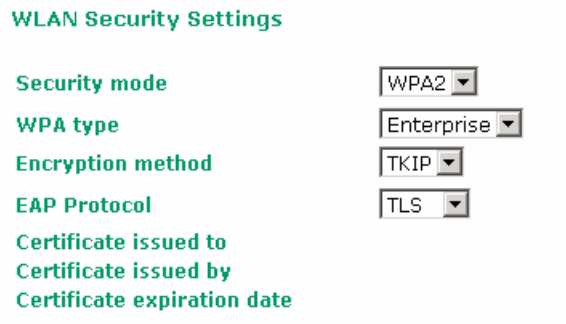
Setting	Description	Factory Default
TLS	Specifies **T**ransport **L**ayer **S**ecurity protocol	TLS
TTLS	Specifies **T**unneled **T**ransport **L**ayer **S**ecurity	
PEAP	Specifies **P**rotected **E**xtensible **A**uthentication **P**rotocol, or *Protected EAP*	

Before choosing the EAP protocol for your WPA/WPA2-Enterpise settings on the client end, please contact the network administrator to make sure the system supports the protocol on the AP end. Detailed information on these three popular EAP protocols is presented in the following sections:

EAP-TLS

TLS is the standards-based successor to the Secure Socket Layer (SSL). It can establish a trusted communication channel over a distrusted network. TLS provides mutual authentication through certificate exchange. EAP-TLS is also secure to use. You are required to submit a digital certificate to the authentication server for validation, but the authentication server must also supply a certificate.

You can use **Basic Wireless Settings** → **WLAN Certificate Settings** to import your WLAN certificate and enable EAP-TLS on the client end.



You can check the current certificate status in ***Current Status*** if it is available.

Certificate issued to: shows the certificate user

Certificate issued by: shows the certificate issuer

Certificate expiration date: indicates when the certificate gets invalid

EAP-TTLS

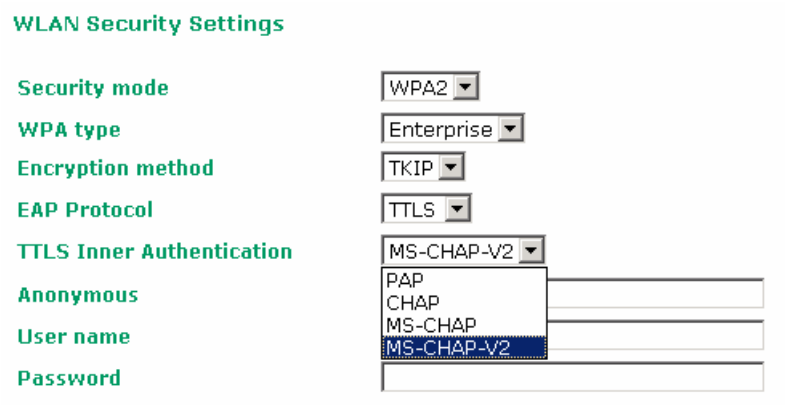
It is usually much easier to re-use existing authentication systems, such as a Windows domain or Active Directory, LDAP directory, or Kerberos realm, rather than creating a parallel authentication system. As a result, TTLS (Tunneled TLS) and PEAP (Protected EAP) are used to support the use of so-called "legacy authentication methods."

TTLS and PEAP work in a similar way. First, they establish a TLS tunnel, like EAP-TLS, and validate whether the network is trustworthy with digital certificates on the authentication server. This step is run to establish a tunnel that protects the next step (or "inner" authentication) so it is sometimes referred to as the "outer" authentication. Then the TLS tunnel is used to encrypt an older authentication protocol that authenticates the user for the network.

As you can see, digital certificates are still needed for the outer authentication in a simplified form. Only a small number of certificates are required, which can be generated by a small certificate authority. Certificate reduction makes TTLS and PEAP much more popular than EAP-TLS.

The AWK-4121 provides some non-cryptographic EAP methods including **PAP**, **CHAP**, **MS-CHAP**, and **MS-CHAP-V2**. These EAP methods are not recommended for direct use on wireless networks. However, they may be useful as inner authentication methods with TTLS or PEAP.

Because the inner and outer authentications can use distinct user names in TTLS and PEAP, you can use an anonymous user name for the outer authentication, while the true user name is shown only through the encrypted channel. Remember, not all client software supports anonymous altercation. Confirm this with the network administrator before you enable identity hiding in TTLS and PEAP.



TTL Inner Authentication

Setting	Description	Factory Default
PAP	**P**assword **A**uthentication **P**rotocol is used	MS-CHAP-V2
CHAP	**C**hallenge **H**andshake **A**uthentication **P**rotocol is used	
MS-CHAP	Microsoft CHAP is used	
MS-CHAP-V2	Microsoft CHAP version 2 is used	

Anonymous

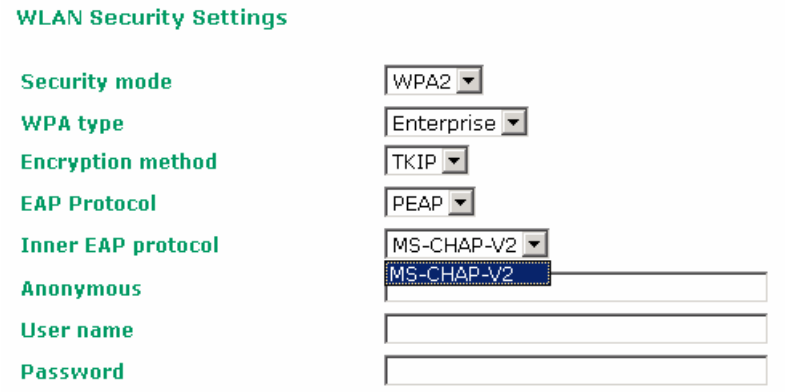
Setting	Description	Factory Default
Max. 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

PEAP

There are a few differences in the inner authentication procedures for TTLS and PEAP. TTLS uses the encrypted channel to exchange attribute-value pairs (AVPs), while PEAP uses the encrypted channel to start a second EAP exchange inside of the tunnel. The AWK-4121 provides **MS-CHAP-V2** merely as an EAP method for inner authentication.



Inner EAP protocol

Setting	Description	Factory Default
MS-CHAP-V2	Microsoft CHAP version 2 is used	MS-CHAP-V2

Anonymous

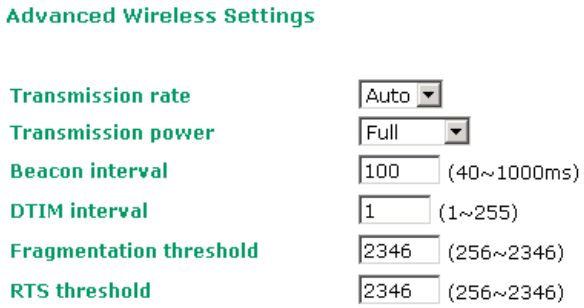
Setting	Description	Factory Default
Max. 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

Advanced Wireless Settings

Additional wireless-related parameters are presented in this section to help you set up your wireless network in detail.



Transmission Rate

Setting	Description	Factory Default
Auto	The AWK-4121 will sense and adjust the data rate automatically	Auto
Available rates	User can manually select a target transmission data rate	

Transmission Power

Setting	Description	Factory Default
Auto	Specifies wireless signal coverage by automatically selecting the strength of Tx power	Full
Full	Equivalent to 100% of maximum Tx power	
High	Equivalent to 75% of maximum Tx power	
Medium	Equivalent to 50% of maximum Tx power	
Low	Equivalent to 25% of maximum Tx power	

***Beacon Interval* (for AP mode only)**

Setting	Description	Factory Default
Beacon Interval (40-1000 ms)	This value indicates the frequency interval of the beacon	100 (ms)

***DTIM Interval* (for AP mode only)**

Setting	Description	Factory Default
Data Beacon Rate (1-16384)	This value indicates how often the AWK-4121 sends out a Delivery Traffic Indication Message	1

Fragment threshold

Setting	Description	Factory Default
Fragment Length (256-2346)	This parameter specifies the maximum size a data packet before splitting and creating another new packet	2346

RTS threshold

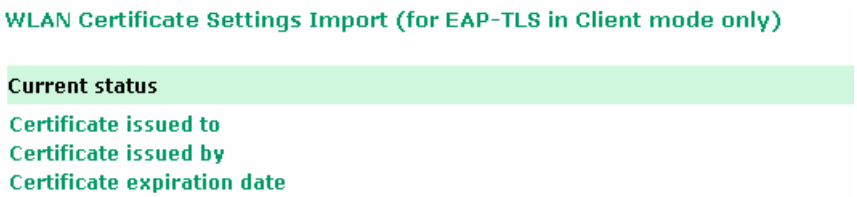
Setting	Description	Factory Default
RTS/CTS Threshold (256-2346)	This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication	2346

NOTE

You can refer to the related glossaries in Chapter 5 for more detailed information about the above-mentioned settings. By setting these parameters properly, you can better tune the performance of your wireless network.

WLAN Certification Settings (for EAP-TLS in Client mode only)

When EAP-TLS is used, a WLAN Certificate will be required at the client end to support WPA/WPA2-Enterprise. The AWK-4121 can support the **PKCS #12**, also known as *Personal Information Exchange Syntax Standard*, certificate formats that define file formats commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.


WLAN Certificate Settings Import (for EAP-TLS in Client mode only)
Current status
Certificate issued to
Certificate issued by
Certificate expiration date

Current status displays information for the current WLAN certificate, which has been imported into the AWK-4121. Nothing will be shown if no certificate is available.

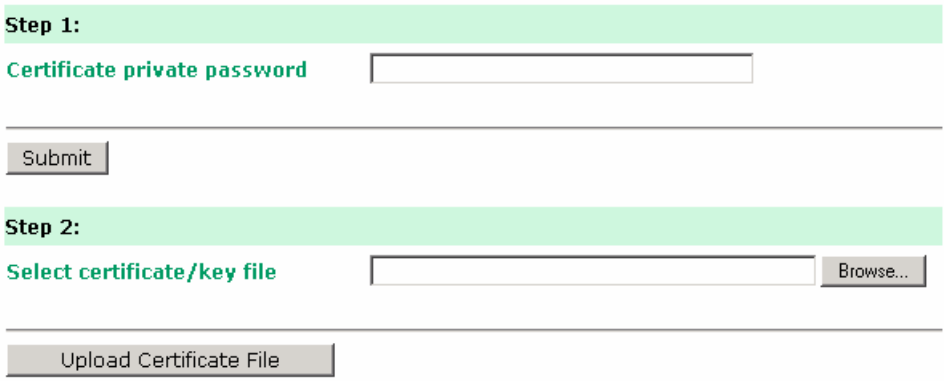
Certificate issued to: shows the certificate user

Certificate issued by: shows the certificate issuer

Certificate expiration date: indicates when the certificate gets invalid

You can import a new WLAN certificate in ***Import WLAN Certificate*** by following these steps in order:

1. Input the corresponding password (or key) in the **Certificate private password** field. Then click **Submit** to set the password.
2. You can see the password displayed in the Certificate private password field. Then click on the **Browse** button in ***Select certificate/key file*** and select the certificate file.
3. Click **Upload Certificate File** to import the certificate file. If it succeeds, you can see the information uploaded in ***Current Certificate***. If it fails, you may need to return to step 1 to set the password correctly and then import the certificate file again.



NOTE

The WLAN certificate will remain after the AWK-4121 reboots. Even though it is expired, it can still be seen on ***Current Certificate***.

Advanced Settings

Several advanced functions are available to increase the functionality of your AWK-4121 and wireless network system. The DHCP server helps you deploy wireless clients efficiently. Packet filters provide security mechanisms, such as firewalls, in different network layers. Moreover, the AWK-4121 can support STP/RSTP protocol to increase the reliability across the entire network. In additional, SNMP support can ease the network management via SNMP protocols.

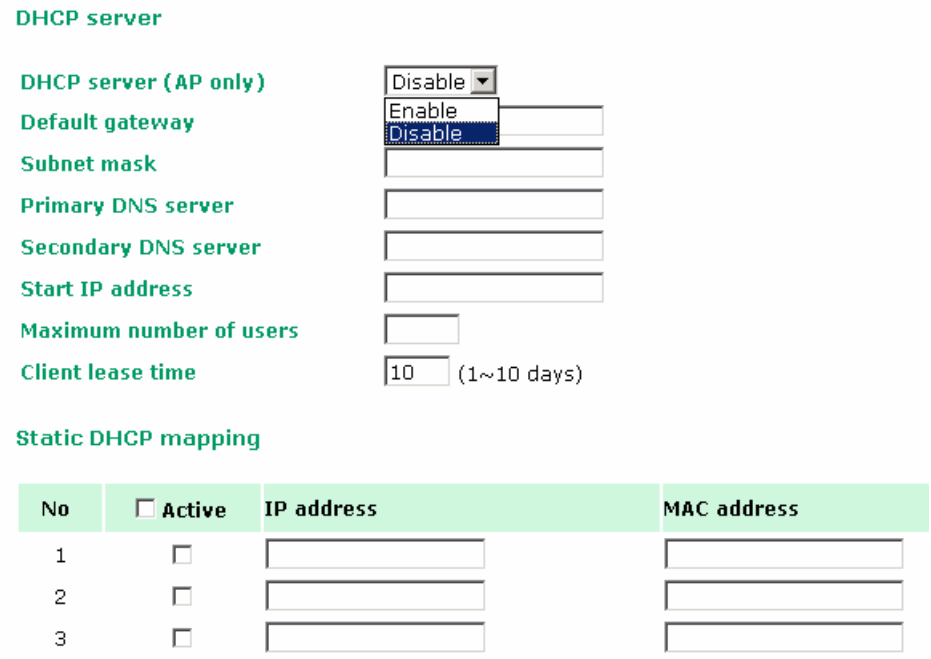
DHCP Server **(for AP mode only)**

DHCP (Dynamic Host Configuration Protocol) is a networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

The AWK-4121 can act as a simplified DHCP server and easily assign IP addresses to your wireless clients by responding to the DHCP requests from the client ends. The IP-related parameters you set on this page will also be sent to the client.

You can also assign a static IP address to a specific client by entering its MAC address. The AWK-4121 provides a **Static DHCP mapping** list with up to 16 entities. Be reminded to check the **Active** check box for each entity to activate the setting.

You can check the IP assignment status under **Status** > **DHCP Client List**.



DHCP server (AP only)

Setting	Description	Factory Default
Enable	Enables AWK-4121 as a DHCP server	Disable
Disable	Disable DHCP server function	

Default gateway

Setting	Description	Factory Default
IP address of a default gateway	The IP address of the router that connects to an outside network	None

Subnet mask

Setting	Description	Factory Default
subnet mask	Identifies the type of sub-network (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network)	None

Primary/ Secondary DNS server

Setting	Description	Factory Default
IP address of Primary/ Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can use URL as well. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

Start IP address

Setting	Description	Factory Default
IP address	Indicates the IP address which AWK-4121 can start assigning	None

Maximum number of users

Setting	Description	Factory Default
1 – 999	Specifies how many IP address can be assigned continuously	None

Client lease time

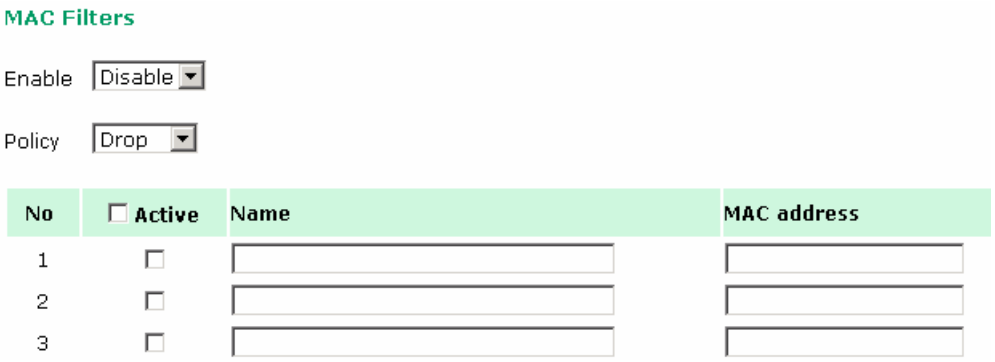
Setting	Description	Factory Default
1 – 10 days	The lease time for which an IP address is assigned. The IP address may go expired after the lease time is reached.	10 (days)

Packet Filters

The AWK-4121 includes various filters for **IP-based** packets going through LAN and WLAN interfaces. You can set these filters as a firewall to help enhance network security.

MAC Filter

The AWK-4121's MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The AWK-4121 provides 8 entities for setting MAC addresses in your filtering policy. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables MAC filter	Disable
Disable	Disables MAC filter	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on list can be allowed.	Drop
Drop	Any packet fitting the entities on list will be denied.	

ATTENTION

Be careful when you enable the filter function:

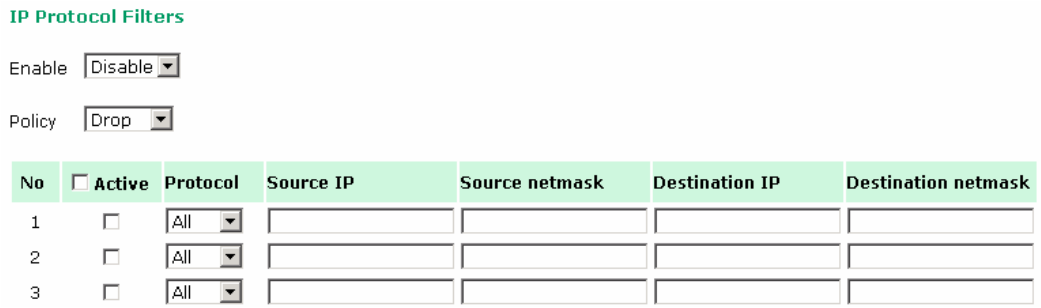
Drop + "no entity on list is activated" = all packets are **allowed**

Accept + "no entity on list is activated" = all packets are **denied**

IP Protocol Filter

The AWK-4121's IP protocol filter is a policy-based filter that can allow or filter out IP-based packets with specified IP protocol and source/destination IP addresses.

The AWK-4121 provides 8 entities for setting IP protocol and source/destination IP addresses in your filtering policy. Four IP protocols are available: **All**, **ICMP**, **TCP**, and **UDP**. You must specify either the Source IP or the Destination IP. By combining IP addresses and netmasks, you can specify a single IP address or a range of IP addresses to accept or drop. For example, "IP address 192.168.1.1 and netmask 255.255.255.255" refers to the sole IP address 192.168.1.1. "IP address 192.168.1.1 and netmask 255.255.255.0" refers to the range of IP addresses from 192.168.1.1 to 192.168.255. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables IP protocol filter	Disable
Disable	Disables IP protocol filter	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on the list can be allowed	Drop
Drop	Any packet fitting the entities on the list will be denied	

ATTENTION

Be careful when you enable the filter function:

Drop + "no entity on list is activated" = all packets are **allowed.**

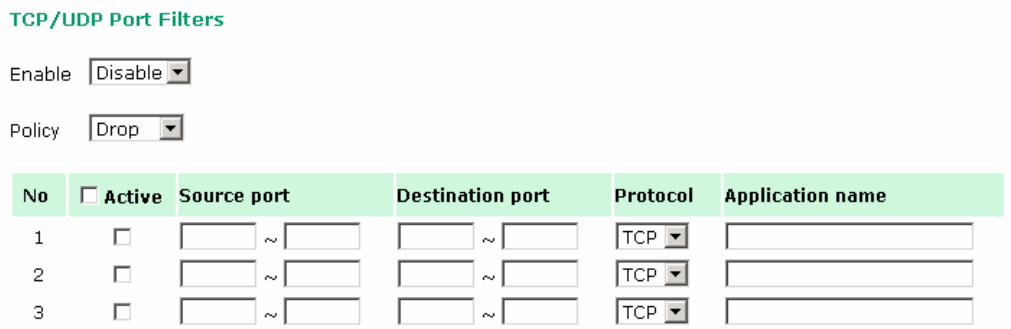
Accept + "no entity on list is activated" = all packets are **denied.**

TCP/UDP Port Filter

The AWK-4121's TCP/UDP port filter is a policy-based filter that can allow or filter out TCP/UDP-based packets with a specified source or destination port.

The AWK-4121 provides 8 entities for setting the range of source/destination ports of a specific protocol. In addition to selecting TCP or UDP protocol, you can set either the source port, destination port, or both. The end port can be left empty if only a single port is specified. Of course, the end port cannot be larger then the start port.

The **Application name** is a text string that describes the corresponding entity with up to 31 characters. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables TCP/UDP port filter	Disable
Disable	Disables TCP/UDP port filter	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on list can be allowed.	Drop
Drop	Any packet fitting the entities on list will be denied.	

ATTENTION

Be careful when you enable the filter function:

Drop + "no entity on list is activated" = all packets are **allowed**

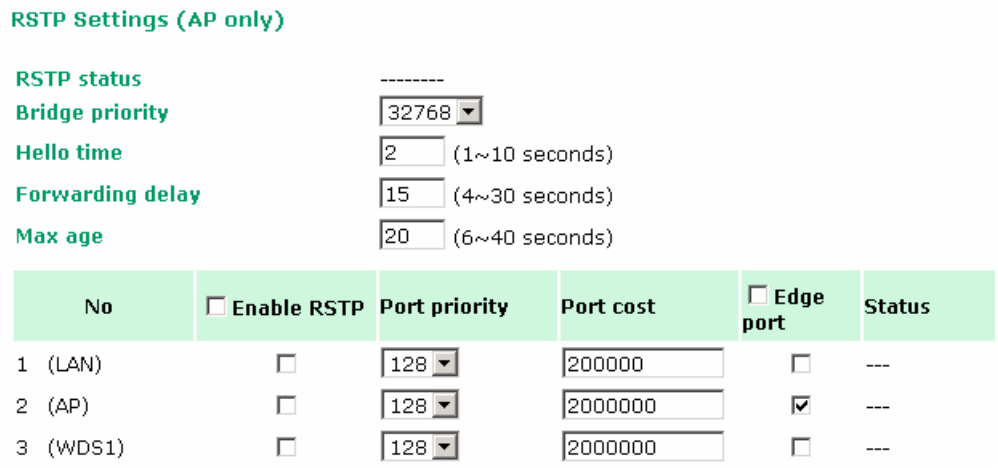
Accept + "no entity on list is activated" = all packets are **denied**

RSTP Settings **(for AP mode only)**

AWK-4121 supports IEEE802.1D Spanning Tree Protocol and IEEE802.1w Rapid STP standards. In addition to eliminating unexpected path looping, STP/RSTP can provide a backup path recovery if a wired/ wireless path fails accidentally. The reliability and availability can increase because this fail-over function.

AWK-4121's STP/RSTP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every AWK-4121 connected to your network. If AWK-4121 plays a **Client** role, which is connected to a device (PLC, RTU, etc.) as opposed to network switch equipment, it is not necessary to enable STP/RSTP. The reason is that it will cause unnecessary negotiation. AWK-4121s support STP/RSTP in **AP** mode (including WDS) only.

The following figures indicate which Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter is given below the figure.



RSTP status

This field will appear only when selected to operate STP/RSTP. It indicates whether this AWK-4121 is the Root of the Spanning Tree (the root is determined automatically) or not.

Bridge priority

Setting	Description	Factory Default
Numerical value selected by user	You can increase the bridge priority by selecting a lower number. A higher bridge priority brings a greater chance of being established as the root of the Spanning Tree topology.	32768

Hello time

Setting	Description	Factory Default
Numerical value input by user (1 – 10 seconds)	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. ***Hello time*** indicates how often the root sends hello messages.	2 (seconds)

Forwarding delay

Setting	Description	Factory Default
Numerical value input by user (4 – 30 seconds)	The amount of time this device waits before checking to see if it should change to a different topology.	15 (seconds)

Max. age

Setting	Description	Factory Default
Numerical value input by user (6 – 40 seconds)	As a non-root role, if the device has not received a hello message from the root longer than ***Max. age***, it will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20 (seconds)

The AWK-4121 comes with 10 "ports" for RSTP settings. Numbers 3-10 (WDS1-WDS8) are available only when WDS is enabled in AP mode.

Enable RSTP

Setting	Description	Factory Default
Enable/ disable	Enables or disables the port as a node on the Spanning Tree topology.	Disable (unchecked)

Port priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by inputting a lower number.	128

Port cost

Setting	Description	Factory Default
Enable/ Disable	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology	2000000

Edge port

Setting	Description	Factory Default
Checked/ unchecked	Sets a port, which no BPDU expectedly goes through, as an edge port	unchecked, except ***AP*** port

NOTE

We recommend you set an edge port for the port, which is connected to a non-STP/RSTP sub-network or an end device (PLC, RTU, etc.) as opposed to network equipment. This can prevent unnecessary waiting and negotiation of STP/RSTP protocol, and accelerate system initialization. When an edge port receives BPDUs, it can still function as an STP/RSTP port and start negotiation.

Setting an edge port is different from disabling STP/RSTP on a port. If you disable STP/RSTP, a port will not deal with STP/RSTP BPDUs at all.

Port Status

Port Status indicates the current Spanning Tree status of this port. Use **Forwarding** for normal transmission, or **Blocking** to block transmission.

SNMP Agent

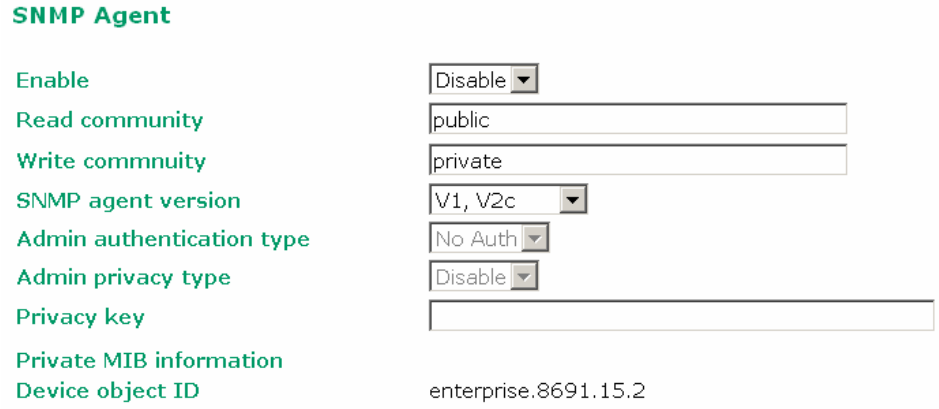
The AWK-4121 supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string *public*/*private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

The AWK-4121's MIB can be found in the software CD and supports reading the attributes via SNMP. (Only ***get*** method is supported.)

SNMP security modes and security levels supported by the AWK-4121 are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	Setting on UI web page	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

The following parameters can be configured on the **SNMP Agent** page. A more detailed explanation of each parameter is given below the following figure.



Enable

Setting	Description	Factory Default
Enable	Enables SNMP Agent	Disable
Disable	Disables SNMP Agent	

***Read community* (for V1, V2c)**

Setting	Description	Factory Default
V1, V2c Read Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can access all objects with read-only permissions using this community string.	public

***Write community* (for V1, V2c)**

Setting	Description	Factory Default
V1, V2c Read /Write Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can accesses all objects with read/write permissions using this community string.	private

SNMP agent version

Setting	Description	Factory Default
V1, V2c, V3, or V1, V2c, or V3 only	Select the SNMP protocol version used to manage the switch.	V1, V2c

***Admin auth type* (for V1, V2c, V3, and V3 only)**

Setting	Description	Factory Default
No Auth	Use **admin** account to access objects. No authentication	No Auth
MD5	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	
SHA	Provides authentication based on HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	

***Admin private key* (for V1, V2c, V3, and V3 only)**

Setting	Description	Factory Default
Disable	No data encryption	Disable
DES	DES-based data encryption	
AES	AES-based data encryption	

Private key

A data encryption key is the minimum requirement for data encryption (maximum of 63 characters)

Private MIB Information Device Object ID

Also know as ***OID***. This is the AWK-4121's enterprise value. It is fixed.

Auto Warning Settings

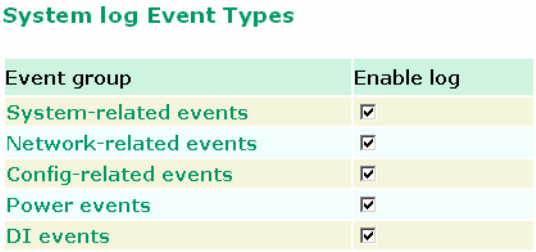
Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. Even when system administrators are out of the control room for an extended period, they can still be informed of the status of devices almost instantaneously when exceptions occur.

In addition to logging these events, the AWK-4121 supports different approaches to warn engineers automatically, such as SNMP trap, e-mail, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

System Log

System Log Event Types

Detail information for grouped events is shown in the following table. You can check the box for **Enable log** to enable the grouped events. All default values are enabled (checked). The log for system events can be seen in **Status > System Log**.



System-related events	Event is triggered when…
System restart (warm start)	The AWK-4121 is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
Network-related events	**Event is triggered when…**
LAN link on	The LAN port is connected to a device or network.
LAN link off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Client joined/ left **(for AP mode)**	A wireless client is associated or disassociated.
WLAN connected to AP **(for Client mode)**	The AWK-4121 is associated with an AP.
WLAN disconnected **(for Client mode)**	The AWK-4121 is disassociated from an AP.
Config-related events	**Event is triggered when…**
Configuration Changed	A configuration item has been changed.
Configuration file import via Web Console	The configuration file is imported to the AWK-4121.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The AWK-4121's firmware is updated.

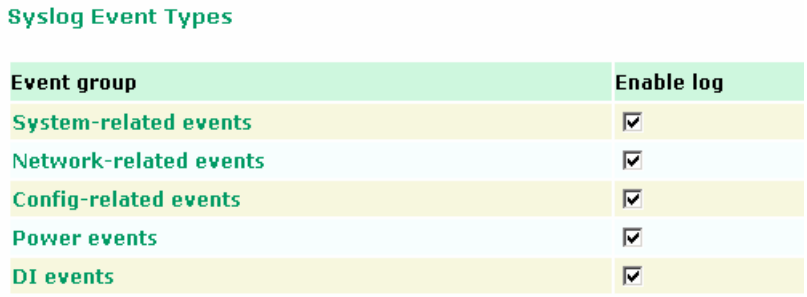
Power events	Event is triggered when…
Power 1/2 transition (On -> Off)	The AWK-4121 is powered down in PWR1/2.
PoE transition (On -> Off)	The AWK-4121 is powered down in PoE.
Power 1/2 transition (Off -> On)	The AWK-4121 is powered via PWR1/2.
PoE transition (Off -> On)	The AWK-4121 is powered via PoE.
DI events	**Event is triggered when…**
DI1/2 transition (On -> Off)	Digital Input 1/2 is triggered by on to off transition
DI1/2 transition (Off -> On)	Digital Input 1/2 is triggered by off to on transition

Syslog

This function provides the event logs for the Syslog server. The function supports up to three configurable Syslog servers and Syslog server UDP port numbers. When an event occurs, the event will be sent as a Syslog UDP packet to the specified Syslog servers.

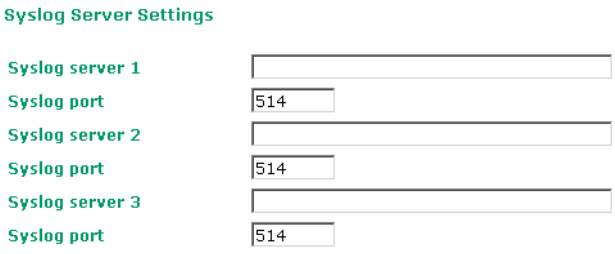
Syslog Event Types

Detail information for the grouped events is shown in the following table. You can check the box for **Enable log** to enable the grouped events. All default values are enabled (checked). Details for each event group can be found on the "System log Event Types" table on page 3-31.



Syslog Server Settings

You can configure the parameters for your Syslog servers in this page.



Syslog server 1/ 2/ 3

Setting	Description	Factory Default
IP address	Enter the IP address of the 1st/ 2nd/ 3rd Syslog Server	None

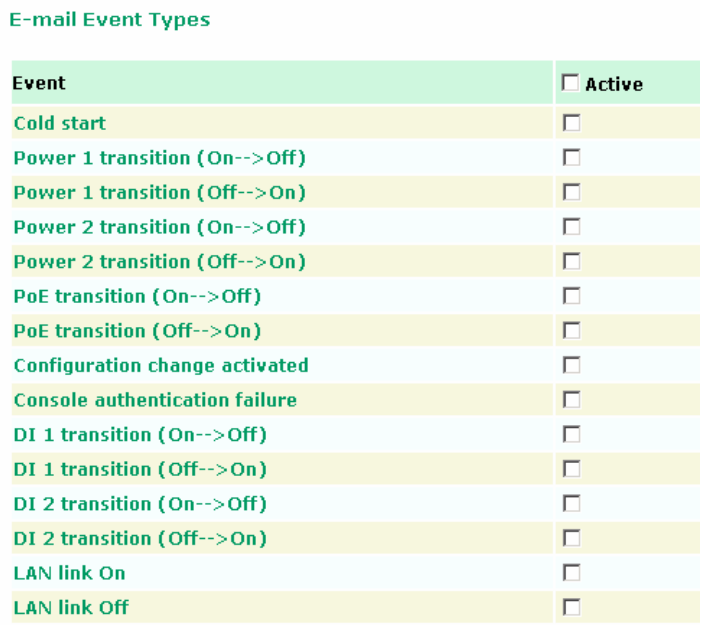
Syslog port

Setting	Description	Factory Default
Port destination (1 to 65535)	Enter the UDP port of the corresponding Syslog server	514

E-mail

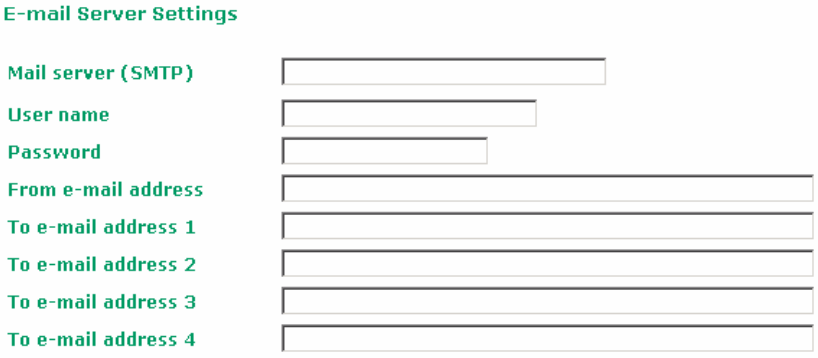
E-mail Event Types

Check the box for **Active** to enable the event items. All default values are deactivated (unchecked). Details for each event item can be found on the "System log Event Types" table on page 3-31.



E-mail Server Settings

You can set up to 4 e-mail addresses to receive alarm emails from the AWK-4121. The following parameters can be configured on the **E-mail Server Settings** page. A more detailed explanation of each parameter is given after the following figure.



Mail server (SMTP)

Setting	Description	Factory Default
IP address	The IP address of your email server.	None

User name & Password

Setting	Description	Factory Default
	User name and password used in the SMTP server	None

From e-mail address

Setting	Description	Factory Default
Max. 63 characters	Enter the administrator's e-mail address which will be shown in the "From" field of a warning e-mail.	None

To E-mail address 1/ 2/ 3/ 4

Setting	Description	Factory Default
Max. 63 characters	Enter the receivers' e-mail addresses.	None

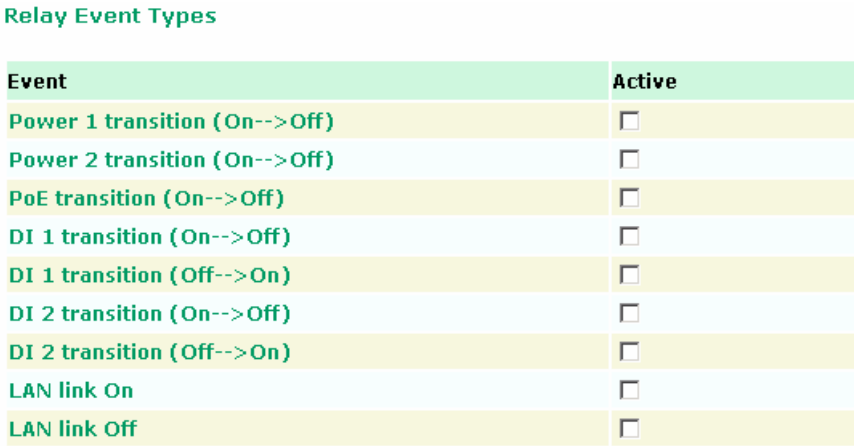
Relay

The AWK-4121 has one relay output, which consists of 2 terminal block contacts on the AWK-4121's top panel. These relay contacts are used to indicate user-configured events and system failure.

The two wires attached to the relay contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the relay circuit will remain closed. For safety reasons, the relay circuit is kept open when the AWK-4121 is not powered.

Relay Event Types

You can check the box for **Active** to enable the event items. All default values are deactivated (unchecked). Details for each event item can be found in the "System log Event Types" table on page 3-31.

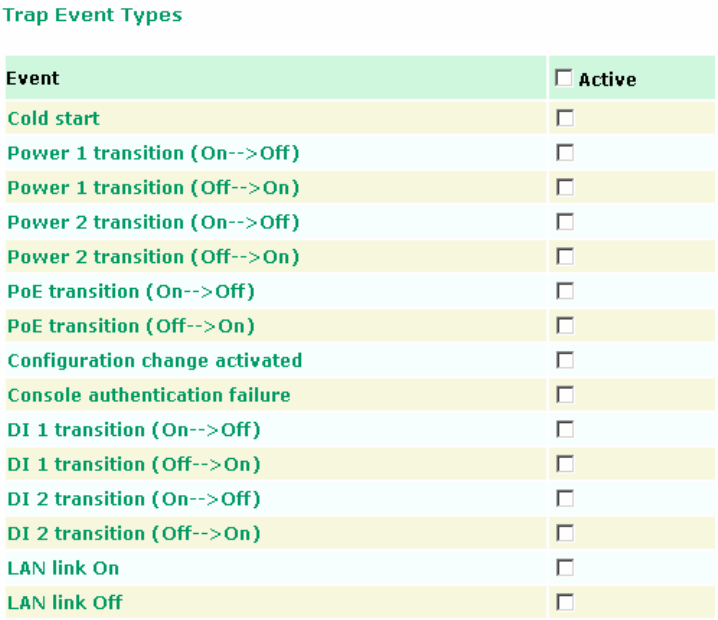


Trap

Traps can be used to signal abnormal conditions (notifications) to a management station. This trap-driven notification can make your network more efficient.

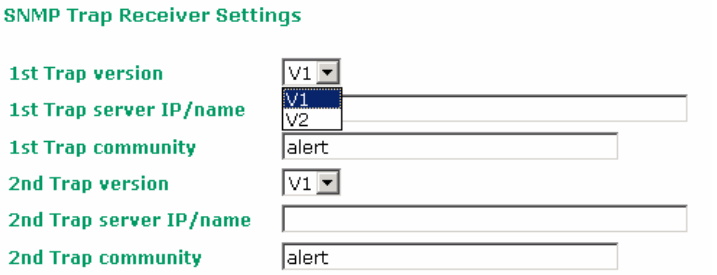
Because a management station usually takes care of a large number of devices that have a large number of objects, it will be overloading for the management station to poll or send requests to query every object on every device. It would be better if the managed device agent could notify the management station by sending a message known as a trap for the event.

Trap Event Types



SNMP Trap Receiver Settings

SNMP traps are defined in SMIv1 MIBs (SNMPv1) and SMIv2 MIBs (SNMPv2c). The two styles are basically equivalent, and it is possible to convert between the two. You can set the parameters for SNMP trap receivers through the web page.



1st / 2nd Trap version

Setting	Description	Factory Default
V1	SNMP trap defined in SNMPv1	V1
V2	SNMP trap defined in SNMPv2	

1st / 2nd Trap server IP/name

Setting	Description	Factory Default
IP address or host name	Enter the IP address or name of the trap server used by your network.	None

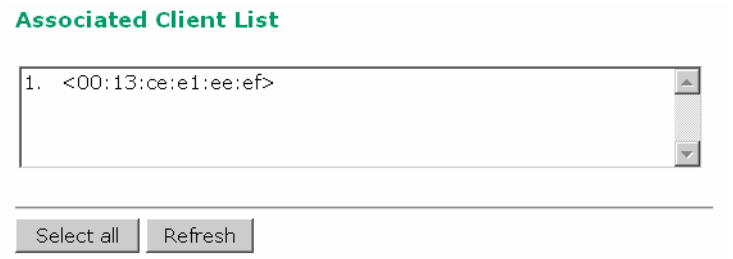
1st / 2nd Trap community

Setting	Description	Factory Default
Max. 31 characters	Use a community string match with a maximum of 31 characters for authentication.	Alert

Status

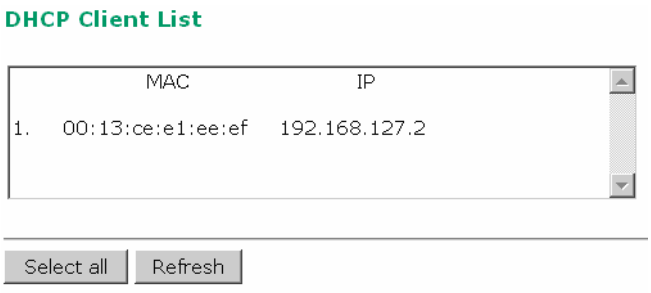
Associated Client List (for AP mode only)

Associated Client List shows all the clients that are currently associated with a specific AWK-4121. You can click **Select all** to select all the content in the list for further editing. You can click **Refresh** to refresh the list.

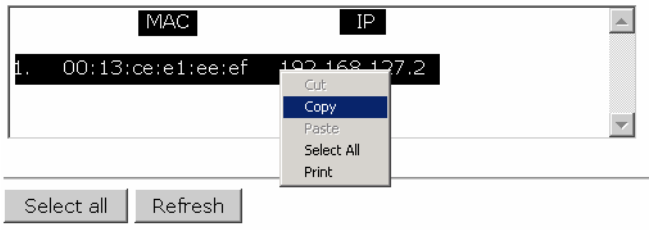


DHCP Client List (for AP mode only)

The DHCP Client List shows all the clients that require and have successfully received IP assignments. You can click the **Refresh** button to refresh the list.

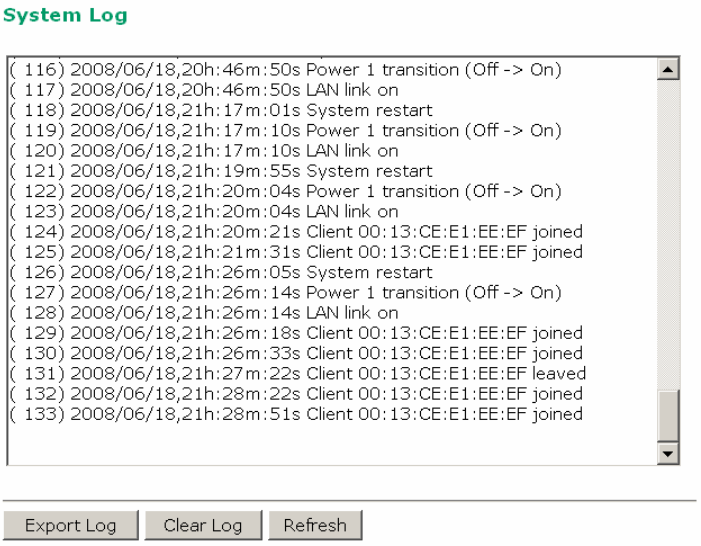


You can press **Select all** button to select all content in the list for further editing.



System Log

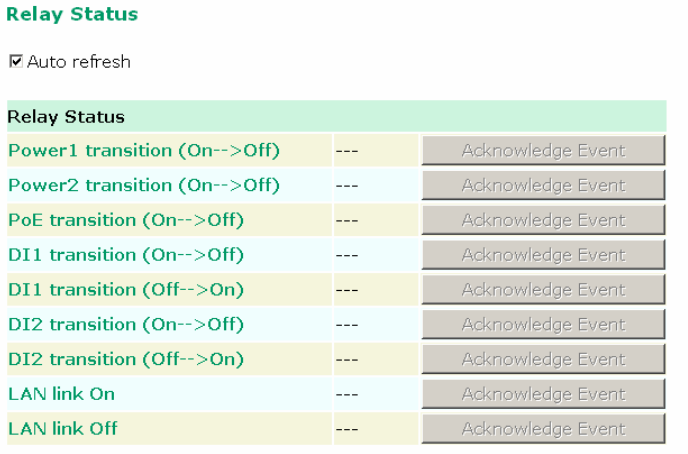
Triggered events are recorded in System Log. You can export the log contents to an available viewer by clicking **Export Log**. You can use the **Clear Log** button to clear the log contents and the **Refresh** button to refresh the log.


System Log
(116) 2008/06/18,20h:46m:50s Power 1 transition (Off -> On)
(117) 2008/06/18,20h:46m:50s LAN link on
(118) 2008/06/18,21h:17m:01s System restart
(119) 2008/06/18,21h:17m:10s Power 1 transition (Off -> On)
(120) 2008/06/18,21h:17m:10s LAN link on
(121) 2008/06/18,21h:19m:55s System restart
(122) 2008/06/18,21h:20m:04s Power 1 transition (Off -> On)
(123) 2008/06/18,21h:20m:04s LAN link on
(124) 2008/06/18,21h:20m:21s Client 00:13:CE:E1:EE:EF joined
(125) 2008/06/18,21h:21m:31s Client 00:13:CE:E1:EE:EF joined
(126) 2008/06/18,21h:26m:05s System restart
(127) 2008/06/18,21h:26m:14s Power 1 transition (Off -> On)
(128) 2008/06/18,21h:26m:14s LAN link on
(129) 2008/06/18,21h:26m:18s Client 00:13:CE:E1:EE:EF joined
(130) 2008/06/18,21h:26m:33s Client 00:13:CE:E1:EE:EF joined
(131) 2008/06/18,21h:27m:22s Client 00:13:CE:E1:EE:EF leaved
(132) 2008/06/18,21h:28m:22s Client 00:13:CE:E1:EE:EF joined
(133) 2008/06/18,21h:28m:51s Client 00:13:CE:E1:EE:EF joined
Export Log
Clear Log
Refresh

Relay Status

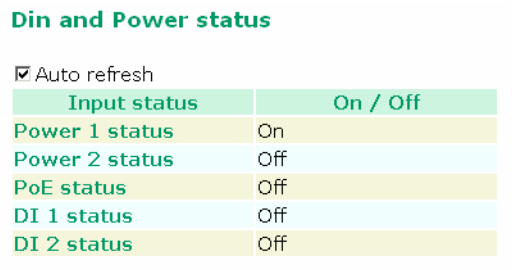
The status of user-configurable events can be found under **Relay Status**. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

If an event is triggered, it will be noted on this list. System administrators can click **Acknowledge Event** when he has acknowledged the event and addressed it.


Relay Status
Auto refresh
Relay Status
Power1 transition (On-->Off) --- Acknowledge Event
Power2 transition (On-->Off) --- Acknowledge Event
PoE transition (On-->Off) --- Acknowledge Event
DI1 transition (On-->Off) --- Acknowledge Event
DI1 transition (Off-->On) --- Acknowledge Event
DI2 transition (On-->Off) --- Acknowledge Event
DI2 transition (Off-->On) --- Acknowledge Event
LAN link On --- Acknowledge Event
LAN link Off --- Acknowledge Event

DI and Power Status

The status of power inputs and digital inputs is shown on this web page. The status will refresh every 5 seconds if the **Auto refresh** box is checked.



Din and Power status

☑ Auto refresh

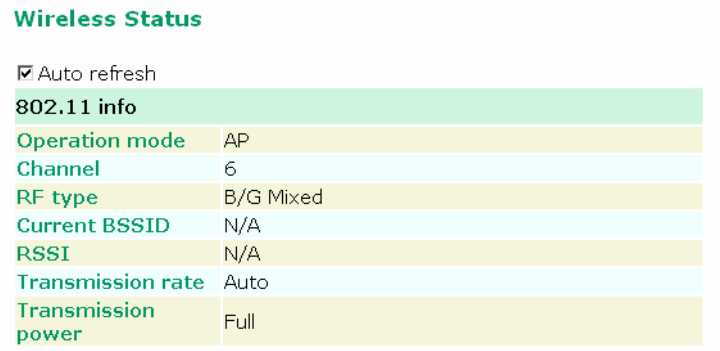
Input status	On / Off
Power 1 status	On
Power 2 status	Off
PoE status	Off
DI 1 status	Off
DI 2 status	Off

Wireless Status

The status for **802.11 info** parameters, such as Operation mode and Channel, are shown on the **Wireless Status** page. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

Certain values for **802.11 info** may not show up due to different operation modes. As a result, **Current BSSID** and **RSSI** are not available in AP mode.

It is helpful to use the continuously updated information on this page, such as RSSI, to monitor the signal strength of the AWK-4121 in Client mode.



Wireless Status

☑ Auto refresh

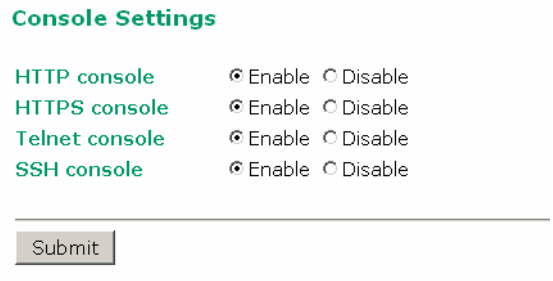
802.11 info	
Operation mode	AP
Channel	6
RF type	B/G Mixed
Current BSSID	N/A
RSSI	N/A
Transmission rate	Auto
Transmission power	Full

Maintenance

Maintenance functions provide the administrator with tools to manage the AWK-4121 and wired/wireless networks.

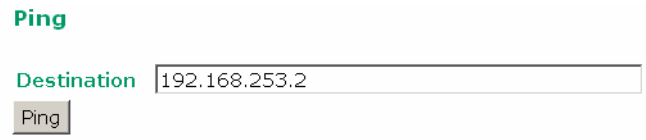
Console Settings

You can enable or disable access permission for the following consoles: HTTP, HTTPS, Telnet and SSH connections. For more security, we recommend you only allow access to the two secured consoles, HTTPS and SSH.

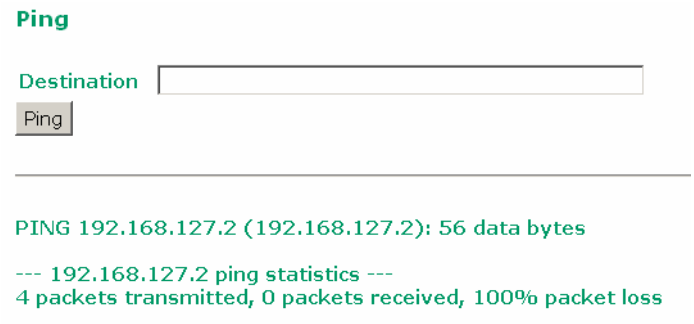


Ping

Ping helps to diagnose the integrity of wired or wireless networks. By inputting a node's IP address in the **Destination** field, you can use the **ping** command to make sure it exists and whether or not the access path is available.



If the node and access path are available, you will see that all packets were successfully transmitted with no loss. Otherwise, some, or even all, packets may get lost, as shown in the following figure.

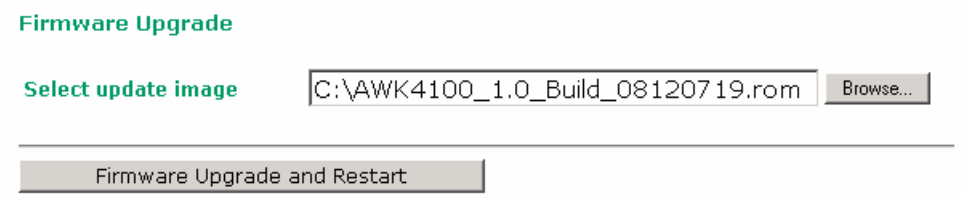


Firmware Upgrade

The AWK-4121 can be enhanced with more value-added functions by installing firmware upgrades. The latest firmware is available at Moxa's download center.

Before running a firmware upgrade, make sure the AWK-4121 is off-line. Click the **Browse** button to specify the firmware image file and click **Firmware Upgrade and Restart** to start the firmware upgrade. After the progress bar reaches 100%, the AWK-4121 will reboot itself.

When upgrading your firmware, the AWK-4121's other functions are forbidden.



ATTENTION

Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup may damage your AWK-4121.

Config Import Export

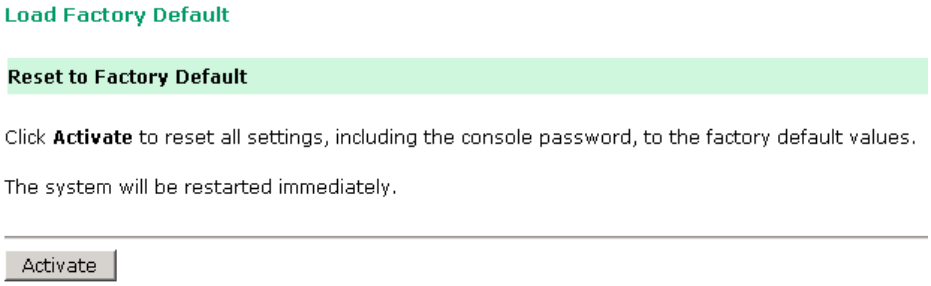
You can back up or restore the AWK-4121's configuration with **Config Import Export**.

In the **Config Import** section, click **Browse** to specify the configuration file and click **Config Import** button to begin importing the configuration.

In the **Config Export** section, click the **Config Export** button and save the configuration file onto your local storage media. The configuration file is a text file and you can view and edit it with a general text-editing tool.

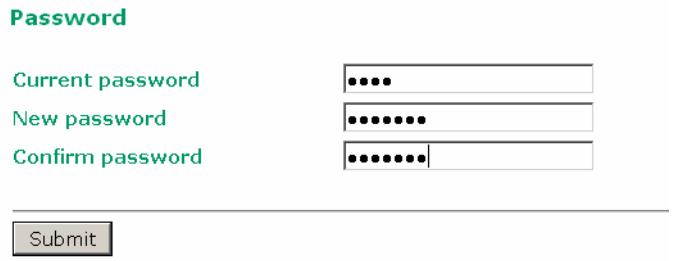
Load Factory Default

Use this function to reset the AWK-4121 and roll all settings back to the factory default values. You can also reset the hardware by pressing the reset button on the top panel of the AWK-4121.


Load Factory Default
Reset to Factory Default
Click Activate to reset all settings, including the console password, to the factory default values.
The system will be restarted immediately.
Activate

Password

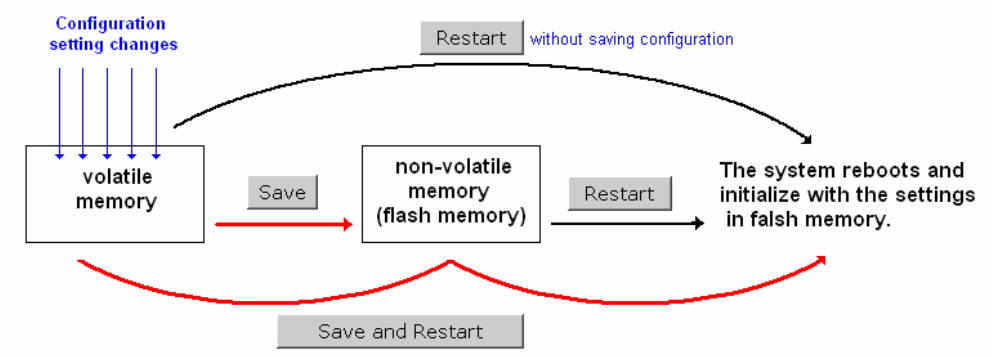
You can change the administration password for each of the AWK-4121's console managers by using the **Password** function. Before you set up a new password, you must input the current password and reenter the new password for confirmation. For your security, do not use the default password ***root***, and remember to change the administration password regularly.



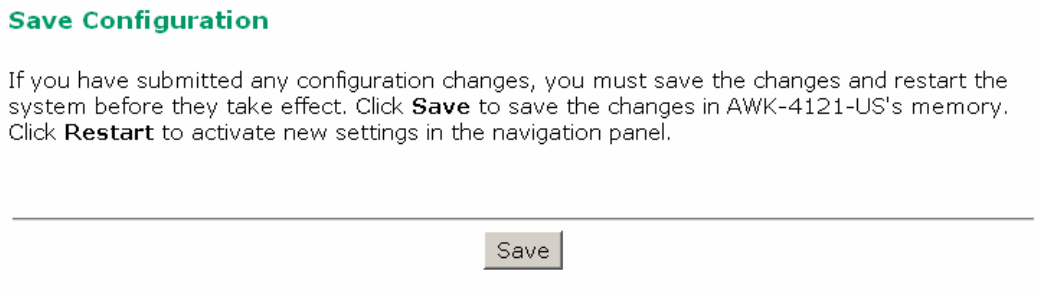
Save Configuration

The following figure shows how the AWK-4121 stores the setting changes into volatile and non-volatile memory. All data stored in volatile memory will disappear when the AWK-4121 is shutdown or rebooted unless they are **y**. Because the AWK-4121 starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the AWK-4121.

This also means the new changes will not work unless you run either the **Save Configuration** function or the **Restart** function.



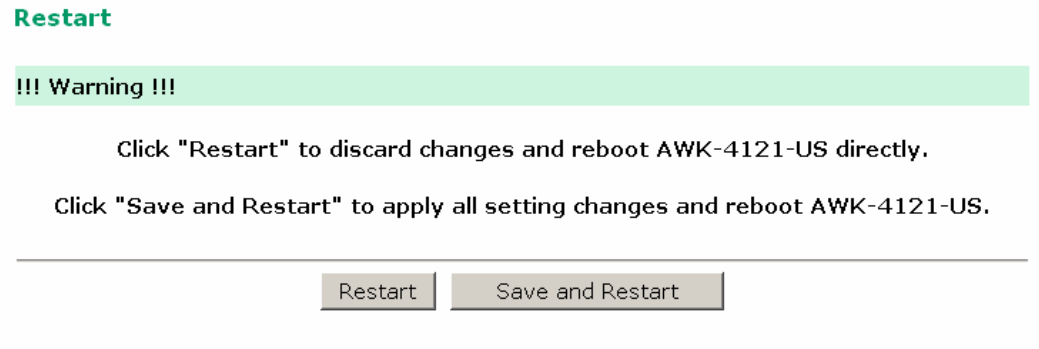
After you click on **Save Configuration** in the left menu box, the following screen will appear. Click **Save** if you wish to update the configuration settings in the flash memory at this time. Alternatively, you may choose to run other functions and put off saving the configuration until later. However, the new setting changes will remain in the non-volatile memory until you save the configurations.


Save Configuration
If you have submitted any configuration changes, you must save the changes and restart the system before they take effect. Click Save to save the changes in AWK-4121-US's memory. Click Restart to activate new settings in the navigation panel.
Save

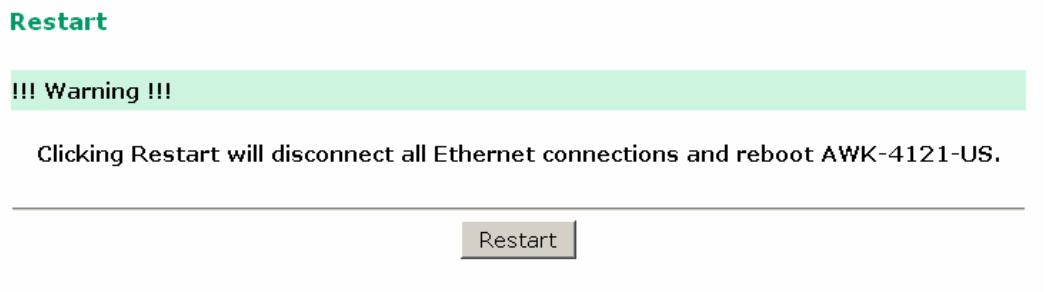
Restart

If you submitted configuration changes, you will find a blinking string in the upper right corner of the screen. After making all your changes, click the **Restart** function in the left menu box. One of two different screens will appear.

If you made changes recently but did not save, you will be given two options. Clicking the **Restart** button here will reboot the AWK-4121 directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the AWK-4121.


Restart
!!! Warning !!!
Click "Restart" to discard changes and reboot AWK-4121-US directly.
Click "Save and Restart" to apply all setting changes and reboot AWK-4121-US.
Restart
Save and Restart

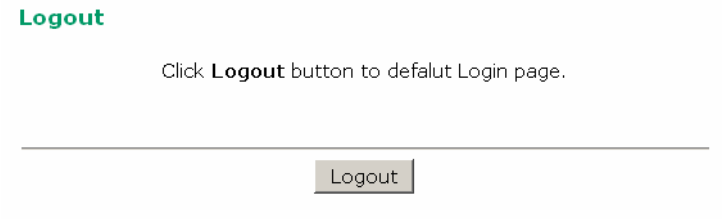
If you run the **Restart** function without changing any configurations or with all changes already saved, you will see just one **Restart** button on your screen.



You will not be able to run any of the AWK-4121's functions while the system is rebooting.

Logout

Logout helps users disconnect the current HTTP or HTTPS session and go to the Login page. For security reasons, we recommend you logout before quitting the console manager.



4

Other Console Configurations

This chapter explains how to access the AWK-4121 for the first time. In addition to HTTP access, there are four ways to access AWK-4121: serial console, Telnet console, SSH console, and HTTPS console. The serial console connection method, which requires using a short serial cable to connect the AWK-4121 to a PC's COM port, can be used if you do not know the AWK-4121's IP address. The other consoles can be used to access the AWK-4121 over an Ethernet LAN, or over the Internet.

In this chapter, we cover the following topics:

- **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- **Configuration by Telnet and SSH Consoles**
- **Configuration by Web Browser with HTTPS/SSL**
- **Disabling Telnet and Browser Access**

ATTENTION

1. You **CANNOT** connect to the AWK-4121 by two ore more of these console configurations simultaneously.
2. You can connect to the AWK-4121 simultaneously by web browser and serial/ Telnet /SSH console. However, we strongly suggest that you do **NOT** use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your AWK-4121.

RS-232 Console Configuration (115200, None, 8, 1, VT100)

The serial console connection method, which requires using a short serial cable to connect the AWK-4121 to a PC's COM port, can be used if you do not know the AWK-4121's IP address. It is also convenient to use serial console configurations when you cannot access the AWK-4121 over Ethernet LAN, such as in the case of LAN cable disconnections or broadcast storming over the LAN.

ATTENTION

Do not use the RS-232 console manager when the AWK-4121 is powered at reversed voltage (ex. -48VDC), even though reverse voltage protection is supported. If you need to connect the RS-232 console at reverse voltage, Moxa's TCC-82 isolator is your best solution.

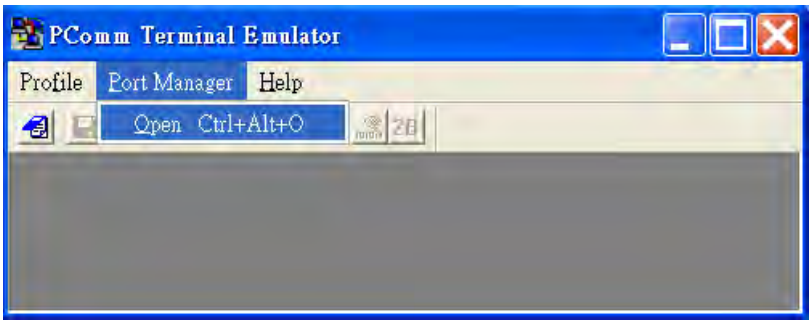
NOTE

We recommend using **Moxa PComm (Lite)** Terminal Emulator, which can be downloaded free of charge from Moxa's website.

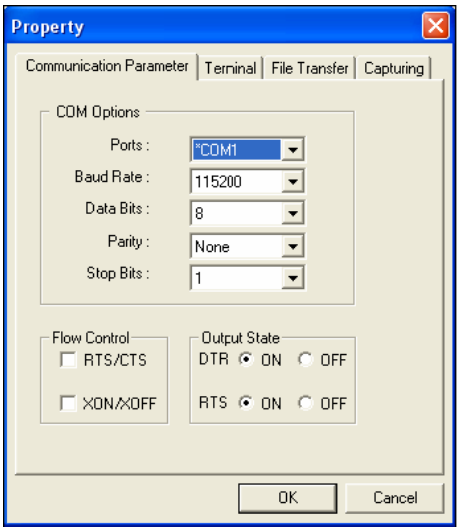
Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the AWK-4121's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing PComm Terminal Emulator, take the following steps to access the RS-232 console utility.

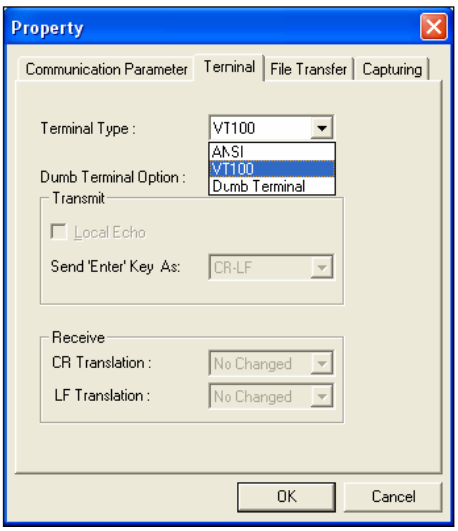
1. From the Windows desktop, open the Start menu and start **PComm Terminal Emulator** in the PComm (Lite) group.

2. Select Open under Port Manager to open a new connection.



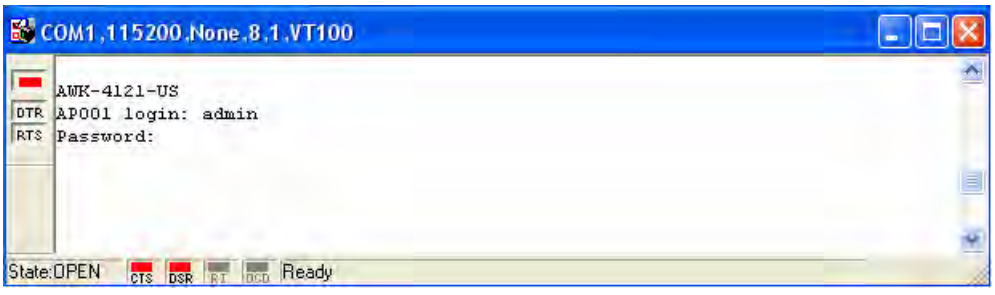
3. The **Communication Parameter** page of the Property window opens. Select the appropriate COM port for Console Connection, **115200** for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits.



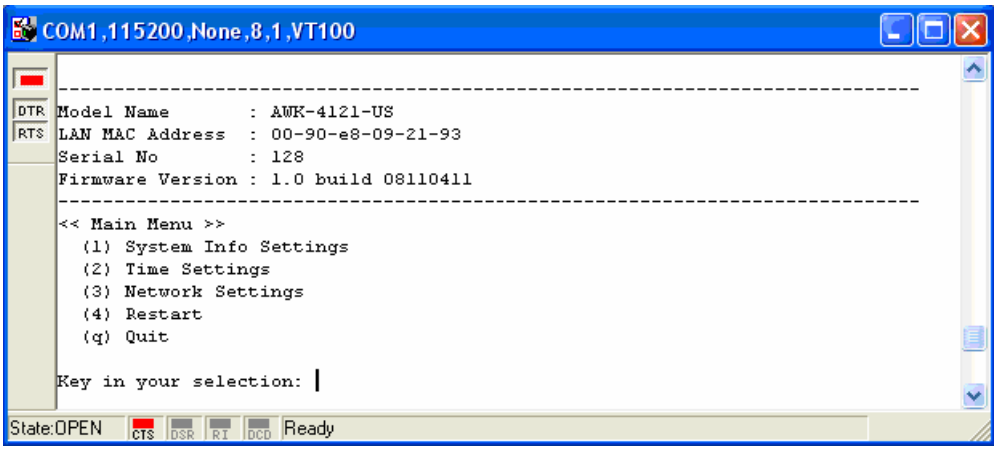


4. Click on the **Terminal** tab, and select **VT100 (or ANSI)** for Terminal Type. Click on **OK** to continue.

5. The Console login screen will appear. Log into the RS-232 console with the login name (default: **admin**) and password (default: **root**, if no new password is set).



6. The AWK-4121's device information and Main Menu will be displayed. Please follow the description on screen and select the administration option you wish to perform.



NOTE

To modify the appearance of the PComm Terminal Emulator window, select **Edit** → **Font** and then choose the desired formatting options.

ATTENTION

If you unplug the RS-232 cable or trigger **DTR**, you will automatically be logged out for network security. You will need to log in again to resume operation.

Configuration by Telnet and SSH Consoles

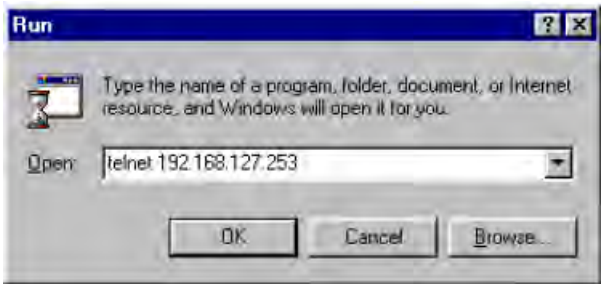
You may use Telnet or SSH client to access the AWK-4121 and manage the console over a network. To access the AWK-4121's functions over the network from a PC host that is connected to the same LAN as the AWK-4121, you need to make sure that the PC host and the AWK-4121 are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

NOTE

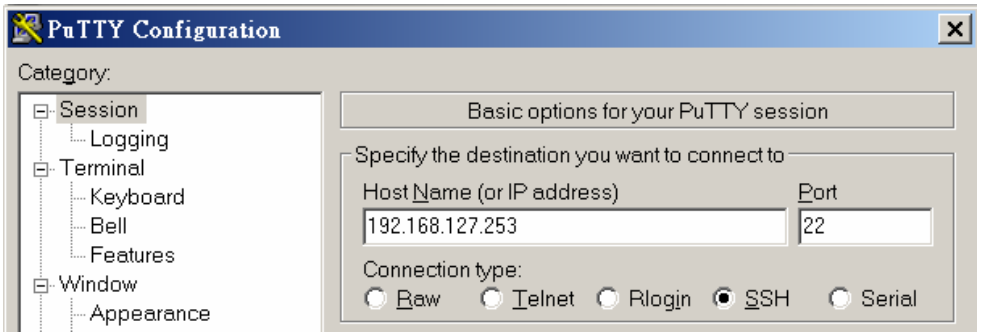
The AWK-4121's default IP address is **192.168.127.253** and the default subnet mask is **255.255.255.0** (for a Class C network). If you do not set these values properly, please check the network settings of your PC host and then change the IP address to 192.168.127.xxx and subnet mask to 255.255.255.0.

Follow the steps below to access the console utility via Telnet or SSH client.

1. From Windows Desktop, run **Start → Run**, and then use Telnet to access the AWK-4121's IP address from the Windows Run window. (You may also issue the telnet command from the MS-DOS prompt.)



When using SSH client (ex. PuTTY), please run the client program (ex. putty.exe) and then input the AWK-4121's IP address, specifying **22** for the SSH connection port.

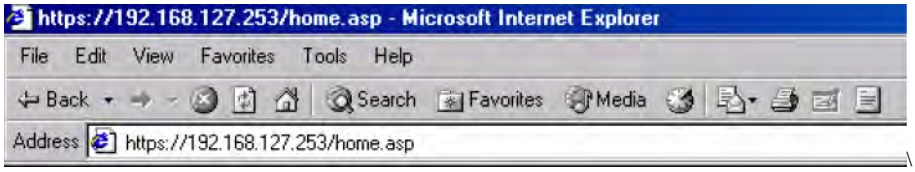


2. The Console login screen will appear. Please refer to the previous paragraph "RS-232 Console Configuration" and for login and administration.

Configuration by Web Browser with HTTPS/SSL

To secure your HTTP access, the AWK-4121 supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the AWK-4121's web browser interface via HTTPS/SSL.

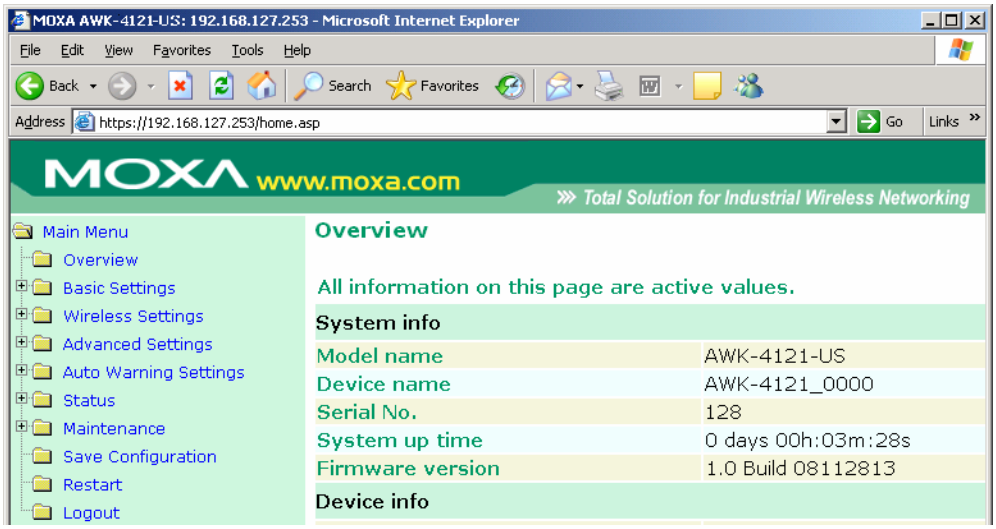
1. Open your web browser and type https://<AWK-4121's IP address> in the address field. Press **Enter** to establish the connection.



2. Warning messages will pop out to warn users that the security certificate was issued by a company they have not chosen to trust.

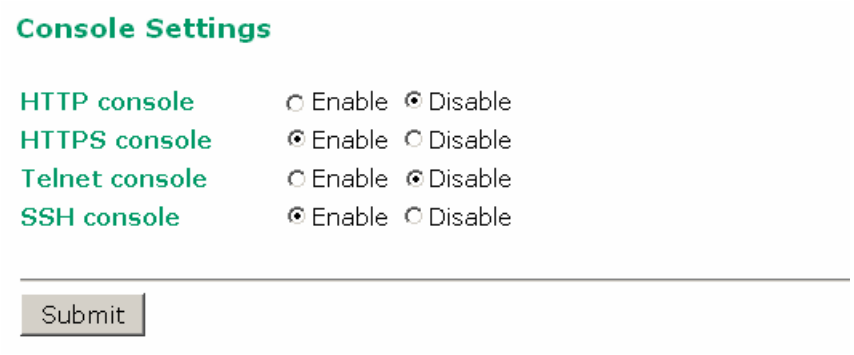
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

3. Select **Yes** to accept the certificate issued by Moxa IW and then enter the AWK-4121's web browser interface secured via HTTPS/SSL. (You can see the protocol in URL is **https**.) Then you can use the menu tree on the left side of the window to open the function pages to access each of the AWK-4121's functions.



Disabling Telnet and Browser Access

If you are connecting the AWK-4121 to a public network but do not intend to use its management functions over the network, then we suggest disabling both Telnet Console and Web Configuration. Please run **Maintenance → Console Settings** to disable them, as shown in the following figure.



5

References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your AWK-4121s and plan your industrial wireless network better.

The following topics are covered:

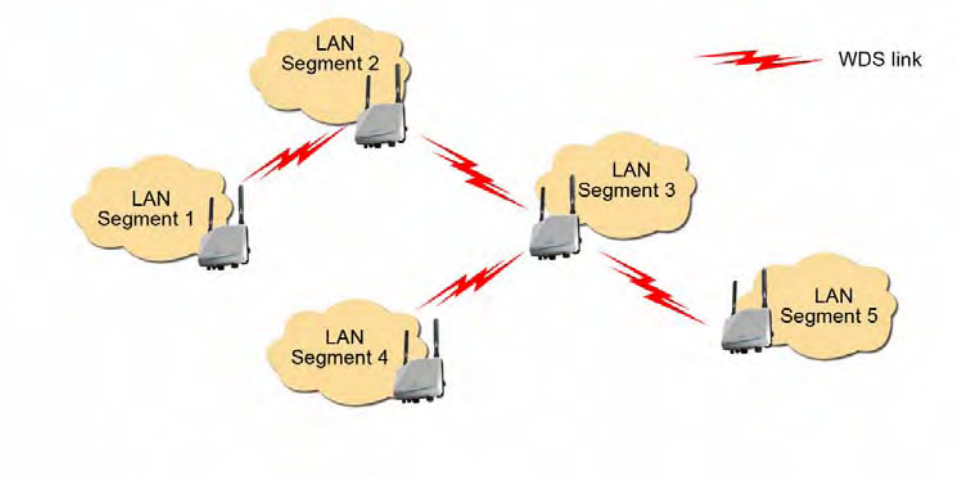
- **Wireless Distribution System (WDS)**
- **Beacon**
- **DTIM**
- **Fragment**
- **RTS Threshold**
- **STP and RSTP**
  - The STP/RSTP Concept
  - Differences between RSTP and STP

Wireless Distribution System (WDS)

Traditionally, APs are connected via Ethernet LAN ports. By using a Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, AP 2 acts as an access point for the notebook computers or other IEEE802.11-enabled clients, and forwards packets sent from the notebook computers to AP 1 through WDS. Then, AP 1 forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the APs to the notebook computers. In this way, AP 2 acts as an "AP repeater."

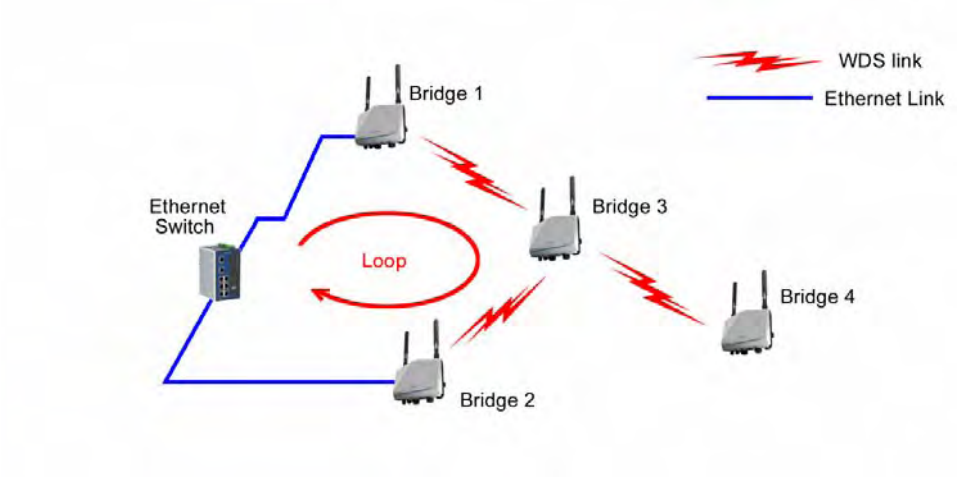
By using WDS, two or more LAN segments can be connected wirelessly. As illustrated in the above figure, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the AP is WDS-enabled, it can be used as a wireless bridge.

It is a good idea to plan your wireless network by drawing a diagram so that you know how each AWK-4121 is connected to other peer APs or wireless bridges by WDS, and how bridges are connected to other peer bridges by WDS. See the following figure for an example of a network-planning diagram.



ATTENTION

Be sure to eliminate loops from networks that consist of wireless bridges, Ethernet switches, Ethernet links, and WDS links. If any loops exist, packets will circle around the loops and network performance will be seriously degraded. The following figure shows a network topology containing a loop.



Beacon

A beacon is a packet broadcast by the AP to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination address, a time stamp, Delivery Traffic Indicator Maps (DTIM), and the Traffic Indicator Message (TIM). Beacon Interval indicates the frequency interval of AP.

DTIM

Delivery Traffic Indication Map (DTIM) is contained in beacon frames. It is used to indicate that broadcast and multicast frames buffered by the AP will be delivered shortly. Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power.

Fragment

A lower setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

RTS Threshold

RTS Threshold (256-2346) – This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of 2,346. When you encounter inconsistent data flow, only minor modifications are recommended.

STP and RSTP

The STP/RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures in a network, and provide protection from loops. Networks that have a complicated architecture are prone to broadcast storms caused by unintended loops in the network. The STP protocol is part of the IEEE802.1D standard, 1998 Edition bridge specification.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE802.1w-2001 standard. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backward compatible with STP, making it relatively easy to deploy. For example:
  - Defaults to sending 802.1D-style BPDUs if packets with this format are received.
  - STP (802.1D) and RSTP (802.1w) can operate on the LAN ports and WLAN ports (AP and WDS1-WDS8) of the same AWK-4121.

This feature is particularly helpful when the AWK-4121 connects to older equipment, such as legacy switches.

Differences between RSTP and STP

RSTP is similar to STP, but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

6

Supporting Information

This chapter presents additional information about this manual and product. You can also learn how to contact Moxa for technical support.

The following topics are covered:

- **About This User's Manual**
- **DoC (Declaration of Conformity)**
  - Federal Communication Commission Interference Statement
  - R&TTE Compliance Statement
- **Firmware Recovery**
- **Technical Support Contact Information**

About This User's Manual

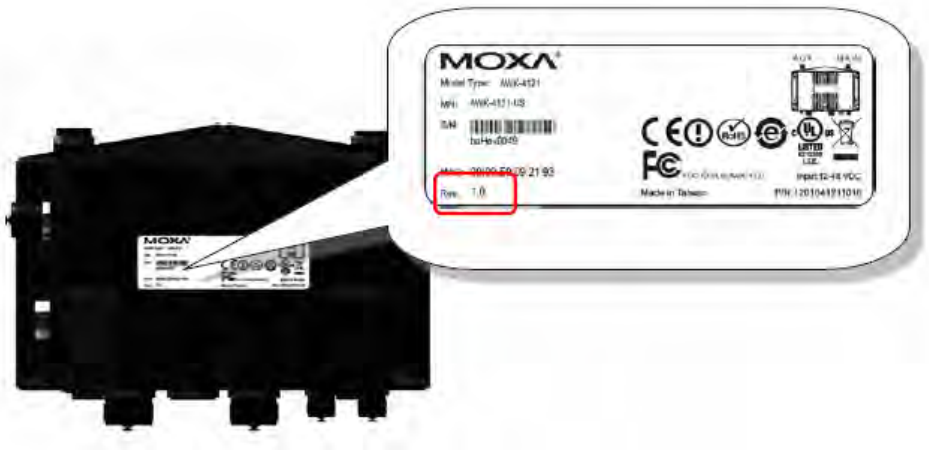
This manual is mainly designed for, but no limited to, the following hardware and firmware for the AWK-4121:

- Hardware Rev: **1.0**
- Firmware Ver: **1.0**

You are strongly recommended to visit Moxa's website (*http://www.moxa.com*) and find the latest product datasheet, firmware, QIG (Quick Installation Guide), UM (User's Manual) and related information.

NOTE

You can find out the hardware revision number of AWK-4121 on the side label.



The firmware version number can be seen on the **Overview** page, as follow:

Overview

All information on this page are active values.

System info	
Model name	AWK-4121-US
Device name	AWK-4121_0000
Serial No.	128
System up time	0 days 00h:03m:28s
Firmware version	1.0 Build 08112813

DoC (Declaration of Conformity)

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Potential Restrictive Use

France: only channels 10, 11, 12, and 13.

Firmware Recovery

When the LEDs of **FAULT**, **Signal Strength**, **CLIENT**, **BRIDGE** and **WLAN** all light up simultaneously and blink at one-second interval, it means the system booting has failed. It may result from some wrong operation or uncontrollable issues, such as an unexpected shutdown during firmware update. The AWK-4121 is designed to help administrators recover such damage and resume system operation rapidly. You can refer to the following instructions to recover the firmware:

Connect to the AWK-4121's ES-232 console with **115200bps and N-8-1**. You will see the following message shown on the terminal emulator every one second.

```
Section userdisk Cksum error = 0xa5feadde --> 0x658c5051
Press Ctrl-C to enter Firmware Recoverying Process.....
Press Ctrl-C to enter Firmware Recoverying Process.....
Press Ctrl-C to enter Firmware Recoverying Process.....
Press Ctrl-C to enter Firmware Recoverying Process.....
Press Ctrl-C to enter Firmware Recoverying Process.....
Press Ctrl-C to enter Firmware Recoverying Process.....
Press Ctrl-C to enter Firmware Recoverying Process.....
Press Ctrl-C to enter Firmware Recoverying Process.....
```

Press **Ctrl - C** and the following message will appear.

```
Press Ctrl-C to enter Firmware Recoverying Process.....
==========================================================================
IP address of AWK-4121 : 0.0.0.0
IP address of TFTP server : 0.0.0.0
==========================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 
```

Enter **2** to change the network setting. Specify where the AWK-4121's firmware file on the TFTP server and press **y** to write the settings into flash memory.

```
==========================================================================
IP address of AWK-4121 : 0.0.0.0
IP address of TFTP server : 0.0.0.0
==========================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 2

IP address of AWK-4121 : 192.168.1.2
IP address of TFTP server : 192.168.1.1
Update RedBoot non-volatile configuration - continue (y/n)? y
```

AWK-4121 restarts, and the "Press Ctrl-C to enter Firmware Recovery Process…" message will reappear. Press **Ctrl-C** to enter the menu and select **1** to start the firmware upgrade process.

```
Press Ctrl-C to enter Firmware Recoverying Process.....
==============================================================================
IP address of AWK-4121 : 192.168.1.2
IP address of TFTP server : 192.168.1.1
==============================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 1
```

Select **0** in the sub-menu to load the firmware image via LAN, and then enter the file name of the firmware to start the firmware recovery.

```
==============================================================================
Load method select :
0. Load from LAN
1. Load from serial with Xmodem
q. Abort select.
==============================================================================
Please select item : 0
Please input load image name..
Default file name : AWK-4121.rom
User Input file name : AWK-4121_1.0.rom
```

Technical Support Contact Information

Customer satisfaction is our number one concern, and to ensure that customers receive the full benefit of our products, Moxa Internet Services has been set up to provide technical support, driver updates, product information, certification status, installation guide and user's manual updates.

The following services are provided:

- E-mail for technical support:

  support@moxa.com (Worldwide)

  support@usa.moxa.com (The Americas)

- World Wide Web (WWW) Site for product information:

  http://www.moxa.com